TABLA DE EQUIVALENCIA FUNCIONAL DE ESTÁNDARES EN MATERIA DE MEDIDAS DE SEGURIDAD EN EL MARCO DE LA LFPDPPP

ifai
Transparencia y Privacidad

ÍNDICE

1. INTRODUCCIÓN A LA NORMATIVIDAD APLICABLE

El 6 de julio de 2010, entró en vigor la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP o la Ley), la cual permite la transferencia legítima, controlada e informada de los datos personales y la protección a la privacidad. También regula el tratamiento de estos datos personales, evitando abusos en su manejo por parte de particulares, sean personas físicas o morales de carácter privado, a quienes la Ley denomina Responsables.

A través de la LFPDPPP se reconocen los derechos de los ciudadanos (denominados en la Ley Titulares) para proteger su privacidad y se faculta a las personas para que puedan solicitar al responsable, en cualquier momento,el acceso rectificación, cancelación u oposición respecto de los datos personales que le conciernen. Derivado de lo anterior, el tratamiento de datos personales está sujeto al consentimiento de su Titular.

Por su parte, todos los particulares como empresas, organizaciones no gubernamentales, organizaciones no lucrativas, entre otros, tienen la obligación de informar a través del aviso de privacidad a los Titulares de los datos qué se recaba de ellos y con qué fines. La Ley establece como violatorio que no se cumpla con la solicitud de acceso, rectificación, cancelación u oposición al tratamiento de los datos personales del ciudadano, así como actuar con negligencia o dolo en el tratamiento de los mismos. También sanciona a quien recabe o transfiera estos datos sin el consentimiento expreso del Titular, y prohíbe la creación de bases de datos en contravención de dicha Ley.

La Ley faculta al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) a regular su aplicación y a establecer sanciones que van desde 100 a 320 mil días de salario mínimo vigente en el Distrito Federal a los responsables que hagan mal uso de la información. En caso de reincidir, se impondrá un castigo adicional similar al anterior, además de que podrán incrementarse hasta por dos veces los montos establecidos cuando se trate de datos sensibles.

Asimismo, se impondrán penas corpóreas de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo custodia. Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o persona autorizada para transmitirlos.

A continuación se indica, de manera comprensible y simplificada, los ordenamientos que ratifican y detallan la obligación a cargo del responsable y encargado de establecer, mantener y documentar las medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales, así como las posibles consecuencias en caso de incumplimiento.

1.1 Constitución Política de los Estados Unidos Mexicanos.

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 16, otorga el carácter de garantía fundamental al derecho a la protección de los datos personales. Lo anterior al establecer que toda persona tiene el derecho a la protección, al acceso, la rectificación y cancelación, y a manifestar su oposición al tratamiento de sus datos personales en los términos que fije la Ley.

1.2 Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

La LFPDPPP regula el derecho a la protección de datos personales a fin de que esta información, en posesión de los responsables, tenga un tratamiento legítimo, controlado e informado. Por lo tanto, la Ley comprende reglas, requisitos, condiciones y obligaciones mínimas para lograr el tratamiento adecuado de los datos personales en posesión de los responsables, sin que esto se traduzca en la imposición de barreras para el desarrollo de las actividades económicas del país.

El artículo 14 de la Ley establece que tanto el responsable como el encargado están obligados a observar el cumplimiento de los principios de protección de datos personales (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad), y por lo tanto deben establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, lo cual se encuentra previsto en el artículo 19 de esta Ley.

De igual manera, el artículo 20 de la Ley establece que las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento de los datos personales que afecten de forma significativa los derechos patrimoniales o morales de las personas, deben ser informadas de forma inmediata por el responsable, a fin de que los titulares de esta información puedan tomar las acciones correspondientes para la defensa de sus derechos.

El artículo 63 de la Ley establece que las siguientes conductas llevadas a cabo por el responsable son sujetas a infracción:

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales.
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.
III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable.

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la Ley.
V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la Ley.
VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.
VII. Incumplir el deber de confidencialidad establecido en el artículo 21 de la Ley.
VIII. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12 de la Ley.
IX. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.
X. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.
XI. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley.
XII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.
XIII. Obstruir los actos de verificación de la autoridad.
XIV. Recabar datos en forma engañosa y fraudulenta.
XV. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.
XVI. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;
XVII. Crear bases de datos en contravención a lo dispuesto por el artículo 9 de la Ley.
XVIII. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la Ley.

Así mismo, en caso de incurrir en alguna de las conductas mencionadas en su artículo 63, la LFPDPPP establece en su artículo 64 las siguientes sanciones:

I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por la Ley.
II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo 63 de la Ley.
III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo 63 de la Ley.
IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. Tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Los artículos 67 y 68 de la Ley tratan de los delitos en materia del tratamiento indebido de datos personales y en los que se menciona lo siguiente:

- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Finalmente, en caso de que se involucren datos personales sensibles, las penas anteriormente mencionadas podrán verse duplicadas.

1.3 Reglamento de la LFPDPPP.

La obligación citada en el artículo 14 de la Ley se reitera en el artículo 47 de su Reglamento, el cual establece que para cumplir con la obligación de proteger y responder por el tratamiento de los datos personales, los responsables y encargados podrán hacer uso de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determinen adecuado para tales fines.

En este sentido, el artículo 48 del Reglamento de la Ley señala que el responsable deberá adoptar medidas para lograr el debido tratamiento de los datos personales, privilegiando los intereses del titular y la expectativa razonable de privacidad. Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:

I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable.
II. Implementar un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.
III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.
IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad.
V. Implementar un procedimiento para que se atienda el riesgo para la protección de datos personales por la adopción de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.
VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.
VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.
VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.

IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.
X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

La obligación establecida en el artículo 19 de la Ley se reitera en el artículo 57 y en la fracción IX del artículo 48 de su Reglamento, y señala que el responsable y el encargado deben establecer medidas para el aseguramiento de los datos personales. Asimismo, el artículo 60 del Reglamento de la Ley estipula que el responsable debe determinar las medidas de seguridad aplicables a los datos personales que trate, considerando factores como:

I. El riesgo.
II. La sensibilidad de los datos personales tratados.
III. El desarrollo tecnológico.
IV. Las posibles consecuencias de una vulneración para los titulares.
V. El número de titulares.
VI. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento.
VII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados por una tercera persona no autorizada para su posesión.
VIII. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

El artículo 61 del Reglamento de la Ley estipula que a fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento.
II. Determinar las funciones y obligaciones de las personas que traten datos personales.
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.
VII. Llevar a cabo revisiones o auditorías.
VIII. Capacitar al personal que efectúe el tratamiento.
IX. Realizar un registro de los medios de almacenamiento de los datos personales.

El artículo 62 del Reglamento de la Ley destaca la obligación de los responsables de actualizar la relación de las medidas de seguridad cuando ocurran los siguientes eventos:

I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.
II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.
III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.
IV. Exista una afectación a los datos personales distinta a las anteriores.

En los artículos 63 al 66 del Reglamento de la Ley se establecen las obligaciones del responsable en caso de ocurrir vulneraciones a la seguridad de los datos personales en cualquier fase del tratamiento. De ser el caso, el responsable deberá informar al titular en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

2. IMPORTANCIA DE LA TABLA DE EQUIVALENCIA

2.1 Definición.

La Tabla de Equivalencia es un material de referencia para los responsables y encargados que les permitirá evaluar si la implementación de determinados estándares internacionales en materia de seguridad de la información y privacidad en su organización facilitan el cumplimiento de los requisitos y obligaciones que establece la Ley y su Reglamento en lo relativo a medidas de seguridad, así como las Recomendaciones en materia de Seguridad de los Datos Personales emitidas por el Instituto.

2.2 Beneficios.

Las ventajas de la Tabla de Equivalencia son las siguientes:

I. Proporciona el apoyo técnico a los responsables y encargados en la protección de datos personales.
II. Contiene estándares internacionales relacionados con la seguridad de la información y privacidad y de amplia aceptación en las organizaciones mexicanas.
III. Ayuda a determinar si la implementación de los controles que se establecen en los estándares internacionales relacionados con la seguridad de la información y

privacidad facilitan el cumplimiento de las obligaciones y requisitos establecidos por la LFPDPPP.

IV. Facilita a los responsables y encargados el cumplimiento de sus obligaciones en materia de seguridad de los datos personales.

V. Ayuda a disminuir el impacto en cuanto a costos de implementación de la LFPDPPP.

VI. Enriquece el objeto de los esquemas de autorregulación vinculante en materia de protección de datos personales.

VII. Ayuda a que los responsables y encargados demuestren ante el Instituto el cumplimiento de las obligaciones previstas en la LFPDPPP.

3. TABLA DE EQUIVALENCIA DE ALTO NIVEL

A continuación se muestra el nivel de contribución que tienen los estándares internacionales en materia de seguridad de la información y privacidad que son objeto de este estudio, para lograr el cumplimiento de los requisitos contenidos en la Ley, su Reglamento, y los Lineamientos del Aviso de Privacidad.

Para el cálculo del nivel de contribución, se toma como base el total de requisitos de la Ley, su Reglamento, y los Lineamientos del Aviso de Privacidad, que componen a la Tabla de Equivalencia. El nivel de contribución Alto es de 87% o más de cumplimiento, el nivel de contribución Medio es de 60% a menos de 87% de cumplimiento, y el nivel de contribución Bajo es de menos de 60% de cumplimiento.

Simbología del Nivel de Contribución

Estándar	Nivel de Contribución
Recomendaciones en materia de Seguridad de Datos Personales emitidas por el IFAI.	
ISO/IEC 27001 (2005, 2013), Information Technology - Security techniques – Information security management systems – Requirements.	

Estándar	Nivel de Contribución
ISO/IEC 27002 (2005, 2013), Information Technology - Security techniques – Code of practice for security management.	
ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.	
ISO/IEC 27006:2011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.	
ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.	
ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.	
ISO/IEC 20000-1:2011 Information technology - Service management -Part 1: Service management system requirements.	
ISO 22301:2012 Societal security - Business continuity management systems – Requirements.	
ISO 31000:2009, Risk management – Principles and guidelines.	
ISO GUIDE 72, Guidelines for the justification and development of management systems standards.	
ISO GUIDE 73, Risk management – Vocabulary.	
ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.	
BS 10012:2009 Data protection – Specification for a personal information management system.	
NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.	
OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.	
Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.	
Control Objectives for Information and Related Technology (COBIT 4.1).	
Control Objectives for Information and Related Technology (COBIT 5).	
PCI DSS, Payment Card Industry Data Security Standard.	

Estándar	Nivel de Contribución
HIPAA, Health Insurance Portability and Accountability Act.	
SOx, Sarbanes-Oxley Act of 2002.	
ITIL, Information Technology Infrastructure Library.	
The Open Web Application Security Project (OWASP).	
Cloud Security Alliance Cloud Controls Matrix (CCM).	

4. SECCIONES

A continuación se muestran los objetivos de control de cada estándar internacional en materia de seguridad de la información y privacidad, que tienen una contribución para lograr el cumplimiento de las obligaciones contenidas en la Ley, su Reglamento, y los Lineamientos de Avisos de Privacidad.

4.1 Recomendaciones en materia de Seguridad de Datos Personales emitidas por el IFAI.

Introducción. Las Recomendaciones en materia de Seguridad de Datos Personales emitidas por el IFAI constituyen un marco de referencia respecto a las acciones que se consideran como las mínimas necesarias para brindar y preservar la seguridad de los datos personales. La Recomendación General es la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		1. Recomendación General.	Recomendación para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) y en estándares internacionales de seguridad de la información y privacidad.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		Paso 1. Establecer el Alcance y los Objetivos.	Los objetivos del Sistema de Gestión de Seguridad de Datos Personales (SGSDP) deben considerar el tratamiento legítimo, controlado e informado de los datos personales.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley, y limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para que los datos personales tratados sean correctos y actualizados.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para limitar el tratamiento de datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					relevantes en relación con las finalidades previstas en el aviso de privacidad.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para el cumplimiento de los principios que establece la Ley: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Lineamientos para que los responsables determinen las características del riesgo sobre los datos personales que tratan.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para el cumplimiento de los principios que establece la Ley: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		Paso 9. Mejora Continua y Capacitación. Capacitación.	Lineamientos para mantener programas de capacitación que mantengan vigente el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		Paso 8. Revisiones y Auditoría. Auditoría.	Lineamientos para contar con un programa de auditoría interna para el monitoreo y revisión de la eficacia y eficiencia del Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	El responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Lineamientos para que los responsables determinen las características del riesgo sobre los datos personales que tratan.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		Paso 8. Revisiones y Auditoría. Auditoría.	Lineamientos para contar con un programa de auditoría interna para el monitoreo y revisión de la eficacia y eficiencia del Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	El responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64		Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	La organización debe contar con procedimientos para el manejo de las vulneraciones de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		1. Recomendación General.	Recomendación para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) y en estándares internacionales de seguridad de la información y privacidad.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para guardar la confidencialidad de los datos personales.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para que los datos personales tratados sean correctos y actualizados.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			1. Recomendación General.	Recomendación para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) y en estándares internacionales de seguridad de la información y privacidad.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Lineamientos para que los responsables determinen las características del riesgo sobre los datos personales que tratan.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		Paso 4. Elaborar un Inventario de Datos Personales.	Lineamientos para establecer y mantener actualizado un inventario de los datos personales que son tratados por la organización.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	El responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Lineamientos para que los responsables determinen las características del riesgo sobre los datos personales que tratan.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	Lineamientos para la selección de controles de seguridad faltantes identificados en el análisis de brecha y en el plan de tratamiento del riesgo.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		Paso 8. Revisiones y Auditoría. Auditoría.	Lineamientos para contar con un programa de auditoría interna para el monitoreo y revisión de la eficacia y eficiencia del Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		Paso 9. Mejora Continua y Capacitación. Capacitación.	Lineamientos para mantener programas de capacitación que mantengan vigente el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		Paso 5. Realizar el Análisis de Riesgo de los Datos Personales. Identificar Activo.	Lineamientos para la identificación de activos relacionados con el ciclo de vida de los datos personales.
Contar con una relación de las medidas de seguridad.		Art. 61		Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Las medidas de seguridad deben seleccionarse con base en el análisis de riesgos y podrán ser tomadas del Anexo D de las Recomendaciones de Seguridad del Instituto (IFAI).

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		Paso 8. Revisiones y Auditoría. Revisión de los Factores de Riesgo.	Lineamientos para el monitoreo y revisión de los riesgos en el contexto del alcance y objetivos del Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	La organización debe contar con procedimientos para el manejo de las vulneraciones de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	La organización debe contar con procedimientos para el manejo de las vulneraciones de seguridad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		1. Recomendación General.	Recomendación para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) y en estándares internacionales de seguridad de la información y privacidad.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		1. Recomendación General.	Recomendación para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar) y en estándares internacionales de seguridad de la información y privacidad.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Medidas de Seguridad.	seguridad.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		Paso 2. Elaborar una Política de Gestión de Datos Personales.	La Política de Gestión de Datos Personales debe contar con reglas para suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de seguridad.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el			Art. 33	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	Designación de un responsable para la rendición de cuentas de la gestión de datos personales y sus responsabilidades para el cumplimiento cotidiano de las medidas de

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.				Medidas de Seguridad.	seguridad.

4.2 ISO/IEC 27001:2013, Information Technology - Security techniques – Information security management systems – Requirements.

Introducción. El estándar proporciona los requerimientos para establecer, controlar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (ISMS: Information Security Management System). La adopción de este sistema de gestión es una decisión estratégica de las organizaciones la cual debe ser basada en los riesgos y objetivos de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
				6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado al cumplimiento de los objetivos de la organización.
				7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
				8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
				9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán	Art. 8	Art. 11		4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de	Art. 14		Art. 15	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado al cumplimiento de los objetivos de la organización.
				7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
				8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
				9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		7.2 Competencia.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad.
				7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		7.1 Recursos.	Asignación de los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora del ISMS.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
				5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el		Art. 50		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
				5.3 Roles, responsabilidades, y autoridades organizacionales.	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a seguridad de la información sean correctamente asignados y comunicados.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
				6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado al cumplimiento de los objetivos de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
				8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
				9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:		Art. 52 - I		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el		Art. 52 - II		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para		Art. 59		5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tal fin.				5.3 Roles, responsabilidades, y autoridades organizacionales.	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a seguridad de la información sean correctamente asignados y comunicados.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
				6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
				5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				5.3 Roles, responsabilidades, y autoridades organizacionales.	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a seguridad de la información sean correctamente asignados y comunicados.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
				8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		7.2 Competencia.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad.
				7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS
				9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos
				10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados		Art. 90	Art. 28	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.					
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.

4.3 ISO/IEC 27002:2013, Information Technology - Security techniques – Code of practice for security management.

Introducción. El ISO 27002:2013 es el código de prácticas de seguridad de la información el cual tiene como objetivo proveer una guía para la implementación de controles para el Sistema de Gestión de Seguridad de la Información ISO 27001.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
				6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
				7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
				8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
				9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
				10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
				11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
				12 Seguridad en las operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
				13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
				14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
				15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
				16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
				17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
				11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
				11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
				12.1.1 Documentación de procedimientos operacionales.	Requerimientos para la documentación formal y comunicación al personal relevante.
				12.3.1 Respaldo de información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que	Art. 14		Art. 15	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
				6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
				7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
guarde alguna relación jurídica.				8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
				9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
				10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
				11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
				12 Seguridad en las operaciones	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
				13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
				14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
				15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
				16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
				17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
				18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
				6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
				7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
				8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
				9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
				11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
				12 Seguridad en las operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
				13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
				14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
				15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
				16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
				17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
				18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		5.1.1 Políticas de Seguridad de la Información.	Actividades y requerimientos para definir un set de políticas relacionadas a la seguridad de la información
				6.2.1 Política de Dispositivos Móviles.	Lineamientos para la implementación de una política para el uso y protección de medios móviles.
				7.2.3 Proceso disciplinario.	Actividades para el establecimiento de un proceso disciplinario en caso de violaciones a la seguridad de la información.
				8.1.3 Uso aceptable de activos.	Establecimiento formal de reglas para el uso aceptable de activos de información.
				9.1.1 Política de Control de Acceso.	Lineamientos para el establecimiento de una política de control de acceso a la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				10.1.1 Política sobre el uso de controles criptográficos.	Aspectos relevantes para el desarrollo de una política sobre el uso de controles criptográficos para protección de la información.
				11.2.9 Política de escritorio y pantalla limpios.	Lineamientos para la implementación de una política de escritorio y pantalla limpios.
				13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
				14.2.1 Política de desarrollo seguro.	Establecimiento formal de políticas de seguridad para el desarrollo de software.
				15.1.1 Política de Seguridad de la Información para el relacionamiento con terceros.	Guía para el establecimiento formal de requerimientos de seguridad cuando se trabaja con proveedores.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la Información.	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la seguridad de la información.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
				18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
				18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		5.1. Dirección de la Gerencia para Seguridad de la Información.	Las actividades para proveer dirección y soporte para la seguridad de la información de acuerdo a los requerimientos del negocio.
				6.1 Organización interna.	Actividades para el establecimiento de un marco para iniciar y controlar la operación de la seguridad de la información.
				18.1 Cumplimiento con requerimientos legales y contractuales.	Actividades para prevenir brechas en cuanto a regulaciones, requerimientos legales, y contractuales.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
				14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
				18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
				18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
				18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
				18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
				18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		12.1.1 Documentación de procedimientos operacionales.	Lineamientos de documentación de procedimientos operacionales y su difusión a las partes relevantes.
				16.1 Gestión de incidentes y mejoras de Seguridad de la Información.	Actividades para la administración de incidentes de seguridad.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		7.2.3 Proceso disciplinario.	Actividades para el establecimiento de un proceso disciplinario en caso de violaciones a la seguridad de la información.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al		Art. 48 - IX		5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.				6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
				7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
				8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
				9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
				10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
				11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
				12 Seguridad en las operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
				13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
				14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
				15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
				16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
				17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
				18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		8.3.1 Gestión de medios removibles.	Lineamientos para la implementación de procedimientos para la gestión de medios removibles.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
				12.7.1 Controles de auditoría sistemas de información.	Actividades para la ejecución de auditorías con el objetivo de minimizar interrupciones en los procesos de negocio.
				13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
				14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		16.1 Gestión de incidentes y mejoras de Seguridad de la Información.	Actividades para la administración de incidentes de seguridad.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.
				15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
				15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.
				18.1 Cumplimiento con requerimientos legales y contractuales.	Lineamientos para prevenir relacionadas a layes y regulaciones o contratos relacionados a seguridad de la información
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		13.2.4 Acuerdos de confidencialidad o de no divulgación.	Requerimientos para el diseño e implementación de acuerdos de confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de información.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			12.3.1 Respaldo de información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
				11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
				12.1.1 Documentación de procedimientos operacionales.	Requerimientos para la documentación formal y comunicación al personal relevante.
				12.3.1 Respaldo de información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			6.1.1 Roles y responsabilidades de Seguridad de la Información.	Todas los roles y responsabilidades deben ser definidos y asignados.
				7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la Información.	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la seguridad de la información.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			6.1.3 Contacto con autoridades.	Se deben mantener contactos con autoridades relacionadas que sean relevantes para la organización.
				6.1.4 Contacto con grupos de interés especial.	Se deben mantener contactos con grupos de interés (especialistas) relacionadas que sean relevantes para la organización.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				13.2.4 Acuerdos de confidencialidad o de no divulgación.	Requerimientos para el diseño e implementación de acuerdos de confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de información.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento;		Art. 52 - I		13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
				13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
				13.2.4 Acuerdos de confidencialidad o de no	Requerimientos para el diseño e implementación de acuerdos de

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				divulgación.	confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de información.
				15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
				15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de		Art. 52 - II		13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.
				15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		6.1.1 Roles y responsabilidades de Seguridad de la Información.	Todas los roles y responsabilidades deben ser definidos y asignados.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
				14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
				8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que será responsable de los mismos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
				8.2.2 Etiquetado de información.	Establece los requerimientos para el etiquetado de información de acuerdo a su clasificación.
Determinar las funciones y obligaciones de las		Art. 61 - II		5.1.1 Políticas de Seguridad de la	Actividades y requerimientos para definir un

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
personas que traten datos personales.				Información.	set de políticas relacionadas a la seguridad de la información
				6.1.1 Roles y responsabilidades de Seguridad de la Información.	Todas los roles y responsabilidades deben ser definidos y asignados.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
				14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal.
				18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma operativa.	Actividades para asegurar que no hay efectos negativos después de haberse realizado cambios en las plataformas operativas.
				18.2 Revisiones de Seguridad de la Información.	Actividades para asegurar que la seguridad de la información se encuentra implementada y operando de acuerdo a las políticas y procedimientos establecidos.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		12.6.1 Gestión de vulnerabilidades técnicas.	Actividades para identificar y prevenir que las vulnerabilidades técnicas en los activos de información sean explotadas.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
				18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
				18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
				18.2.3 Revisión de cumplimiento	Revisiones periódicas sobre el cumplimiento

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				técnico.	de los sistemas de información de acuerdo a las políticas establecidas.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la Información.	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la seguridad de la información.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
				8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que será responsable de los mismos.
				8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
				8.2.2 Etiquetado de información.	Establece los requerimientos para el etiquetado de información de acuerdo a su clasificación.
Contar con una relación de las medidas de seguridad.		Art. 61		8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
				8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que será responsable de los mismos.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		16.1.5 Respuesta a incidentes de Seguridad de la Información.	Procedimientos para la respuesta a incidentes de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		16.1.6 Lecciones aprendidas de los incidentes de Seguridad de la Información.	Establecimiento de una base de datos de eventos de seguridad para minimizar el impacto de eventos similares en el futuro.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
				13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
				13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
				13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		6.1.3 Contacto con autoridades.	Se deben mantener contactos con autoridades relacionadas que sean relevantes para la organización.
				6.1.4 Contacto con grupos de interés especial.	Se deben mantener contactos con grupos de interés (especialistas) relacionadas que sean relevantes para la organización.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
				11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
				12.1.1 Documentación de procedimientos operacionales.	Requerimientos para la documentación formal y comunicación al personal relevante.
				12.3.1 Respaldo de información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades prevenir brechas relacionadas a la seguridad de información personal
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas			Art. 33	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
inicialmente, y el consentimiento del titular sea necesario.					

4.4 ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.

Introducción. Este estándar proporciona lineamientos para la gestión de riesgos de seguridad de la información. Su finalidad es apoyar la implementación de seguridad de la información con base en un enfoque de gestión de los riesgos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		7 Establecimiento del Contexto.	Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información.
				8 Evaluación del Riesgo de Seguridad de la Información.	Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
				12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		NO APLICA	NO APLICA
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		NO APLICA	NO APLICA
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		NO APLICA	NO APLICA
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	7 Establecimiento del Contexto.	Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información
				8 Evaluación del Riesgo de Seguridad de la Información.	Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
				12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
			Art. 38		
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		NO APLICA	NO APLICA
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles	Art. 19	Art. 9 Art. 48		7.1 Consideraciones generales.	Factores de la organización que inciden en la gestión de riesgos de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.				7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
				8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
				8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		NO APLICA	NO APLICA
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
				12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
				12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
				7.3 Límites y alcance.	Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información.
				7.4 Organización para la Gestión del Riesgo de Seguridad de la Información.	Organización y responsabilidades para la gestión del riesgo de seguridad de la información.
				8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
				8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
				12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		12 Monitoreo y revisión de Riesgos de Seguridad de la Información	Acciones para monitorear los riesgos y sus factores en la organización.
				12.1 Monitoreo y revisión de factores de riesgo	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
				12.2 Monitoreo, revisión, y mejora de la gestión del riesgo	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		NO APLICA	NO APLICA
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		NO APLICA	NO APLICA
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
				8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		NO APLICA	NO APLICA
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar	Art. 21	Art. 9		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
sus relaciones con el titular o, en su caso, con el responsable.					
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			NO APLICA	NO APLICA
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán	Art. 44			7.2.1 Enfoque de la Gestión del Riesgo.	Desarrollo de un enfoque de la gestión del riesgo para abordar los criterios de evaluación, impacto, y aceptación de riesgos.
				7.2.2 Criterios de evaluación del Riesgo.	Factores de la organización a considerar para la evaluación del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.				7.2.3 Criterio para el Impacto.	Factores de la organización a considerar para determinar el impacto de los riesgos.
				7.2.4 Criterio para aceptación del Riesgo.	Definición de escalas y niveles de aceptación del riesgo.
				11 Comunicación y consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de		Art. 52 - II		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		NO APLICA	NO APLICA
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		NO APLICA	NO APLICA
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración		Art. 60		7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
				7.3 Límites y alcance.	Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información.
				7.4 Organización para la Gestión del Riesgo de Seguridad de la Información.	Organización y responsabilidades para la gestión del riesgo de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
				8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información
				10 Aceptación del Riesgo de Seguridad de la Información	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
				12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		8.2.2 Identificación de activos	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
				8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
				12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		8.2.2 Identificación de activos.	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.
				8.2.3 Identificación de amenazas.	Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.
				8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
				8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
				8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al negocio por incidentes de seguridad.
				8.3.3 Evaluación de probabilidad de incidente.	Determinación de la probabilidad de un incidente de seguridad.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
				9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		8.2.2 Identificación de activos	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información
				8.2.3 Identificación de amenazas.	Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.
				8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.
				8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
				8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
				8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					negocio por incidentes de seguridad
				8.3.3 Evaluación de probabilidad de incidente.	Determinación de la probabilidad de un incidente de seguridad.
				8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		9.1 Descripción general del Tratamiento del Riesgo.	Lineamientos para el tratamiento del riesgo.
				9.2 Modificación del Riesgo.	Medidas para modificar el riesgo.
				9.3 Retención del Riesgo.	Lineamientos para la retención del riesgo.
				9.4 Cancelación del Riesgo.	Lineamientos para la cancelación del riesgo.
				9.5 Transferencia del Riesgo.	Lineamientos para la trasferencia del riesgo.
				10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
				11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
				12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
				12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		8.2.2 Identificación de activos.	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
				12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
				12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
				8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
				8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al negocio por incidentes de seguridad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		7.2.1 Enfoque de la Gestión del Riesgo.	Desarrollo de un enfoque de la gestión del riesgo para abordar los criterios de evaluación, impacto, y aceptación de riesgos.
				7.2.2 Criterios de evaluación del Riesgo.	Factores de la organización a considerar para la evaluación del riesgo.
				7.2.3 Criterio para el Impacto.	Factores de la organización a considerar para determinar el impacto de los riesgos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.2.4 Criterio para aceptación del Riesgo.	Definición de escalas y niveles de aceptación del riesgo.
				11 Comunicación y consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		7.2.1 Enfoque de la Gestión del Riesgo.	Desarrollo de un enfoque de la gestión del riesgo para abordar los criterios de evaluación, impacto, y aceptación de riesgos.
				7.2.2 Criterios de evaluación del Riesgo.	Factores de la organización a considerar para la evaluación del riesgo.
				7.2.3 Criterio para el Impacto.	Factores de la organización a considerar para determinar el impacto de los riesgos.
				7.2.4 Criterio para aceptación del Riesgo.	Definición de escalas y niveles de aceptación del riesgo.
				11 Comunicación y consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		NO APLICA	NO APLICA
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o			Art. 33	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.					

4.5 ISO/IEC 27006:2011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.

Introducción. Este estándar establece los requerimientos y es una guía para entidades que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información. Su enfoque principal es para ayudar a la acreditación de entidades de certificación de sistemas de gestión de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		NO APLICA	NO APLICA
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		NO APLICA	NO APLICA
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		NO APLICA	NO APLICA
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Establecer un sistema de supervisión y vigilancia		Art. 48 - III		9.1.1.1 Criterios de auditoría de	Establece como criterio de auditoría al

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.				certificación.	utilizado en ISO 27001.
				9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
				9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
				9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
				9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
				9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		7.1.1.1 Análisis de competencias y revisión contractual.	Establece el proceso de revisión de la organización cliente en cuanto a sus riesgos y su competencia en seguridad de la información.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.
				9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
				9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
				9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
				9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
				9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50		8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
				8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal;		Art. 60		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.
				9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
				9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
				9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
				9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
				9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
				9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
				9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
				9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
				9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
				9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Contar con una relación de las medidas de seguridad.		Art. 61		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		NO APLICA	NO APLICA
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas			Art. 33	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
inicialmente, y el consentimiento del titular sea necesario.					

4.6 ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.

Introducción. Este estándar es una guía para la revisión de la implementación y operación de controles, incluyendo la revisión del cumplimiento técnico de controles de sistemas de información, en concordancia con los estándares de seguridad de la información establecidos en la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular.	Art. 8	Art. 11		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.					
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		NO APLICA	NO APLICA
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		NO APLICA	NO APLICA
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado	Art. 14		Art. 15	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
en todo momento por él o por terceros con los que guarde alguna relación jurídica.				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		NO APLICA	NO APLICA
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		NO APLICA	NO APLICA
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		NO APLICA	NO APLICA
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		NO APLICA	NO APLICA
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		NO APLICA	NO APLICA
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.					
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		NO APLICA	NO APLICA
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		NO APLICA	NO APLICA
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			NO APLICA	NO APLICA
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad		Art. 52 - II		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		NO APLICA	NO APLICA
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		NO APLICA	NO APLICA
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará		Art. 60		8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				8.2.5 Hallazgos previos.	Consideraciones del uso de hallazgos previos para la revisión de controles.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		NO APLICA	NO APLICA
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		NO APLICA	NO APLICA
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		NO APLICA	NO APLICA
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		NO APLICA	NO APLICA
Contar con una relación de las medidas de seguridad.		Art. 61		8.1 Preparaciones	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento
				8.2.4 Consideraciones relacionadas a los objetos	Especificación, documentación, y configuración de activos de información y la selección de los métodos de revisión apropiados
				8.2.7 Sistemas externos	Revisión de sistemas de información externos a la organización
				8.2.8 Organización y activos de información	Adaptación de los procesos de revisión para sistemas y plataformas específicas
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de		Art. 62		7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.				7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
				7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
				7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
				8 Actividades.	Actividades de preparación de los controles para su revisión.
				8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
				8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
				8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
				8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		NO APLICA	NO APLICA
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		NO APLICA	NO APLICA
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes.		Art. 90	Art. 28	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.					
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		NO APLICA	NO APLICA
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original,			Art. 33	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.					

4.7 ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.

Introducción. Este estándar internacional provee una estructura general para la protección de información de identificación personal (PII: Personally Identifiable Information). Con el estándar ISO 29100 se pretende ayudar a las organizaciones a definir los mecanismos de protección relacionados a la privacidad de datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		4 Elementos básicos del marco de trabajo de Privacidad.	Describe los componentes básicos relacionados a la privacidad de datos personales para el establecimiento del marco de privacidad.
				5 Los principios de Privacidad de ISO/IEC 29100.	Describe a detalle los principios que deben ser utilizados para el desarrollo de políticas y procedimientos utilizados para la protección de datos personales.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
				5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.4 Límite en la recolección.	Indica las limitantes para la recopilación de datos personales.
				5.5 Minimización de datos.	Define cómo deben ser divulgados los datos personales bajo el principio de la necesidad de saber.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	4.4.7 Información Personal Identificable Sensible.	Características de la información personal sensible de acuerdo al estándar.
				5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		5.7 Precisión y calidad.	Este principio establece que los datos recopilados deben ser exactos, completos y actualizados de acuerdo al propósito para el que sean recopilados.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.4 Límite en la recolección.	Indica las limitantes para la recopilación de datos personales.
				5.5 Minimización de datos.	Define cómo deben ser divulgados los datos personales bajo el principio de la necesidad de saber.
				5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que	Art. 14		Art. 15	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
guarde alguna relación jurídica.					
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		4.5 Requerimientos de protección de la Privacidad.	Provee una definición de los requerimientos de protección de datos personales y los factores que influyen en ellos.
				4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		4.6 Políticas de Privacidad.	Elementos para el diseño y establecimiento de la política de privacidad de una organización.
				5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		4.5 Requerimientos de protección de la Privacidad.	Provee una definición de los requerimientos de protección de datos personales y los factores que influyen en ellos.
				4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
				5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable.		Art. 50		4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
				4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por
				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
				5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			4 Elementos básicos del marco de trabajo de Privacidad.	Describe los componentes básicos relacionados a la privacidad de datos personales para el establecimiento del marco de privacidad.
				5 Los principios de Privacidad de ISO/IEC 29100.	Describe a detalle los principios que deben ser utilizados para el desarrollo de políticas y procedimientos utilizados para la protección de datos personales.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por
				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
				4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
				4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por
				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de		Art. 52 - II		4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
				4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por
				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se		Art. 54		4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
				4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
				4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
				4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
realizó con autorización del responsable corresponderá al encargado.				4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
				4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará		Art. 60		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				5.11 Seguridad de la Información.	|Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Contar con una relación de las medidas de seguridad.		Art. 61		4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		4 Elementos básicos del marco de trabajo de Privacidad.	Describe los componentes básicos relacionados a la privacidad de datos personales para el establecimiento del marco de privacidad.
				5 Los principios de Privacidad de ISO/IEC 29100.	Describe a detalle los principios que deben ser utilizados para el desarrollo de políticas y procedimientos utilizados para la protección de datos personales.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o			Art. 33	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
				5.4 Límite en la recolección.	Indica las limitantes para la recopilación de datos personales.
				5.5 Minimización de datos.	Define cómo deben ser divulgados los datos personales bajo el principio de la necesidad de saber.
				5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.					

4.8 ISO/IEC 20000-1:2011 Information technology - Service management -Part 1: Service management system requirements.

Introducción: ISO 20000 es un estándar orientado al establecimiento de procesos y procedimientos para la gestión de servicios de TI y con ello prevenir los riesgos tecnológicos dentro de la operación de una organización. La gestión de los servicios de tecnología informática es un enfoque integrado basado en procesos que alinea la prestación de servicios de TI con las necesidades de la organización que los presta.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
				4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				4.3 Gestión de documentación.	El proveedor del servicio debe establecer y mantener los documentos, incluyendo los registros, para asegurar la eficaz planificación, operación y control del sistema de gestión de servicios.
				4.4 Gestión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros necesarios.
				4.5 Establecer y mejorar el Sistema de Gestión de Servicios.	El proveedor de servicios debe definir e incluir el alcance del sistema de gestión de servicios en el plan de gestión de servicios.
				5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
				6 Procesos de Entrega de Servicios.	El proveedor de servicios deberá estar de acuerdo a los servicios que se entregarán con el cliente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7 Procesos de Relacionamiento.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8 Procesos de Resolución.	Habrá un procedimiento documentado para todas las incidencias.
				9 Procesos de Control.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el buen funcionamiento del sistema de gestión de servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiado.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el buen funcionamiento del sistema de gestión de servicios.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación.	Art. 14		Art. 15	4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				4.3 Gestión de documentación.	El proveedor del servicio debe establecer y mantener los documentos, incluyendo los registros, para asegurar la eficaz planificación, operación y control del sistema de gestión de servicios.
				4.4 Gestión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros necesarios.
				4.5 Establecer y mejorar el Sistema de Gestión de Servicios.	El proveedor de servicios debe definir e incluir el alcance del sistema de gestión de servicios en el plan de gestión de servicios.
				5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
				6 Procesos de Entrega de Servicios.	El proveedor de servicios deberá estar de acuerdo a los servicios que se entregarán con el cliente.
				7 Procesos de Relacionamiento.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8 Procesos de Resolución.	Habrá un procedimiento documentado para todas las incidencias.
				9 Procesos de Control.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación,

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					formación, habilidades y experiencia.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				4.5.4 Monitoreo y revisión del Sistema de Gestión de Servicios.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		4.4.1 Provisión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros necesarios.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la		Art. 50		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
autoridad competente.					
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			4.1.4 Representante de la Gerencia.	La gerencia debe designar un miembro de la gerencia del proveedor de servicios que, con independencia de otras responsabilidades, tiene las facultades y responsabilidades que incluyen los procesos del sistema de gestión de servicios.
				7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			4 Requerimientos generales del Sistema de Gestión de Servicios.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al		Art. 52 - II		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada		Art. 60		5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.
				4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación, formación, habilidades y experiencia.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.
				4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación,

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					formación, habilidades y experiencia.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
Contar con una relación de las medidas de seguridad.		Art. 61		6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
				8.2 Gestión de Problemas.	Habrá un procedimiento documentado para identificar los problemas y minimizar o evitar el impacto de los incidentes y problemas.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el buen funcionamiento del sistema de gestión de servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
				7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		4 Requerimientos generales del Sistema de Gestión de Servicios.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el		Art. 95		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
acuse de recibo que entregue al titular la correspondiente fecha de recepción.				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
				8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas			Art. 33	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.					

4.9 ISO 22301:2012 Societal security - Business continuity management systems – Requirements.

Introducción. Este estándar especifica los requerimientos para planear, establecer, implementar, operar, supervisar, revisar, mantener, y mejorar de forma continua un sistema documentado de gestión para la protección contra eventos disruptivos en la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
				5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
				6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
				7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
				8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.
				9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
				10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		6.2 Objetivos de continuidad del negocio y planes para alcanzarlos.	Establecimiento de objetivos de continuidad del negocio así como de responsables para su consecución.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
			Art. 37		
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		5.3 Política.	Aspectos fundamentales que debe contener la política de continuidad del negocio de la organización.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		7.3 Concientización.	Concientización de todos los responsables de la organización para cumplir con los objetivos y planes de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.4 Comunicación.	Aspectos a considerar para el intercambio de información relacionada con el sistema de gestión de continuidad del negocio con las partes interesadas.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
				9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
				9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
				7.1 Recursos.	Identificación de recursos necesarios para la implementación del sistema de gestión de continuidad del negocio.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
				9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
				9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		5.1 Liderazgo y compromiso.	Responsabilidades en la organización para lograr los objetivos y planes de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				5.2 Compromiso gerencial.	Responsabilidades de la gerencia para lograr los objetivos y planes de continuidad del negocio.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
				8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			5.4 Roles, responsabilidades, y autoridades organizacionales.	Asignación y comunicación de responsabilidades y autoridades dentro del sistema de gestión de continuidad del negocio.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
				5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
				6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
				7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
				8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.
				9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
				10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
				6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
				6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
				6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		5.4 Roles, responsabilidades, y autoridades organizacionales.	Asignación y comunicación de responsabilidades y autoridades dentro del sistema de gestión de continuidad del negocio.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará		Art. 60		6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
				6.2 Objetivos de continuidad de negocio y planes para alcanzarlos.	Establecimiento de los objetivos de continuidad de negocio de la organización y determinación de acciones y responsables para lograr dichos objetivos.
				8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		5.4 Roles, responsabilidades, y autoridades organizacionales.	Asignación y comunicación de responsabilidades y autoridades dentro del sistema de gestión de continuidad del negocio.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
				8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		10 Mejora.	Acciones para la mejora continua del sistema de gestión de continuidad del negocio.
				10.1 No conformidad y acciones correctivas.	Manejo de no conformidades detectadas en el sistema de gestión de continuidad del negocio.
				10.2 Mejora continua.	Proceso de mejora continua e implementación de correcciones al sistema de gestión de continuidad del negocio.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
				9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
				9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		7.3 Concientización.	Concientización de todos los responsables de la organización para cumplir con los objetivos y planes de continuidad del negocio.
				7.4 Comunicación.	Aspectos a considerar para el intercambio de información relacionada con el sistema de gestión de continuidad del negocio con las partes interesadas.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Contar con una relación de las medidas de seguridad.		Art. 61		8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el		Art. 62		9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.				9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
				9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		NO APLICA	NO APLICA
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los		Art. 69		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales.				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70		4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
				5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
				6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
				7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
				8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.
				9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
				10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
				5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
				6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
				7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
				8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.
				9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
				10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.					
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.10 ISO 31000:2009, Risk management – Principles and guidelines.

Introducción. Este estándar proporciona los principios y las guías genéricas para la gestión de riesgos, por lo que puede ser utilizada por cualquier organización no importando la industria o sector. Los puntos contenidos en este estándar pueden ser aplicados a lo largo de la vida de una organización, y para una diversidad de actividades, incluyendo estrategias y decisiones, operaciones, proceso, funciones, proyectos, productos, servicios, y activos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		2 Términos y definiciones.	Términos y definiciones de la gestión del riesgo.
				3 Principios.	Principios para la gestión efectiva del riesgo.
				4.2 Responsabilidad y compromiso.	Compromiso de la alta dirección de la organización para la gestión efectiva del

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					riesgo.
				4.3 Diseño del marco de trabajo para la Gestión del Riesgo.	Características principales con las que debe contar un marco de trabajo para la gestión del riesgo.
				4.4 Implementación de la Gestión del Riesgo.	Consideraciones para la implementación efectiva de la gestión del riesgo.
				4.5 Monitoreo y revisión del marco de trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
				4.6 Mejora continua del marco de trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
				5.2 Comunicación y consulta.	Comunicación y consulta con las partes interesadas para la gestión efectiva del riesgo.
				5.3 Establecimiento del contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
				5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
				5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
				5.6 Monitoreo y revisión.	Procesos de monitoreo y revisión del riesgo.
				5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		2.26 Control.	Definición y ejemplos de control.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		2.26 Control.	Definición y ejemplos de control.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		2.26 Control.	Definición y ejemplos de control.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	2.26 Control.	Definición y ejemplos de control.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
				5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
				5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		5.3 Estableciendo el contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
				5.3.2 Contexto Externo.	Factores externos de la organización que inciden en la gestión del riesgo.
				5.3.3 Contexto Interno.	Factores internos de la organización que inciden en la gestión del riesgo.
				5.3.4 Estableciendo el contexto del proceso de Gestión del Riesgo.	Elementos necesarios para el establecimiento del contexto del proceso de gestión del riesgo.
				5.3.5 Definición de criterio del Riesgo.	Definición y establecimiento del criterio para evaluar el riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		4.3.2 Estableciendo la Política de Gestión del Riesgo.	Enfoque y elementos de la política de gestión del riesgo.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		NO APLICA	NO APLICA
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
				4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
				5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
				5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
				5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.
				5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
				5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
				5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
				5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
				4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
				5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
				5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			NO APLICA	NO APLICA
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			NO APLICA	NO APLICA
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;		Art. 52 - II		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		NO APLICA	NO APLICA
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		NO APLICA	NO APLICA
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración		Art. 60		5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
				5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
				5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
				5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
				5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		NO APLICA	NO APLICA
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		NO APLICA	NO APLICA
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
				5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.
				5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
				5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
				5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
				5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
				5.6 Monitoreo y revisión.	Procesos de monitoreo y revisión del riesgo.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
				5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
				4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
				5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
				5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		2.26 Control.	Definición y ejemplos de control.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		5.3 Estableciendo el contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
				5.3.2 Contexto Externo.	Factores externos de la organización que inciden en la gestión del riesgo.
				5.3.3 Contexto Interno.	Factores internos de la organización que inciden en la gestión del riesgo.
				5.3.4 Estableciendo el contexto del proceso de Gestión del Riesgo.	Elementos necesarios para el establecimiento del contexto del proceso de gestión del riesgo.
				5.3.5 Definición de criterio del Riesgo.	Definición y establecimiento del criterio para evaluar el riesgo.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
				4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
				5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
				5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		4 Marco de Trabajo.	Aspectos del marco de trabajo para la gestión efectiva del riesgo.
				5 Proceso.	Procesos para la gestión efectiva del riesgo.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		4 Marco de Trabajo.	Aspectos del marco de trabajo para la gestión efectiva del riesgo.
				5 Proceso.	Procesos para la gestión efectiva del riesgo.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		2.26 Control.	Definición y ejemplos de control.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen			Art. 33	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.					

4.11 ISO GUIDE 72, Guidelines for the justification and development of management systems standards.

Introducción. Esta guía proporciona los lineamientos para la justificación y evaluación de un proyecto estándar de un sistema de gestión incluyendo: la visión de la evaluación de relevancia en el mercado, los procesos de desarrollo y mantenimiento con una visión para asegurar su compatibilidad y mejora, y la terminología, estructura, y elementos comunes a ser integrados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
				B2 Planeación.	Procesos de planeación del sistema de gestión.
				B3 Implementación y Operación.	Procesos de implementación y operación del sistema de gestión.
				B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
				B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.
				B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
				B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
				B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
				B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36	B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
			Art. 38		
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
				B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
				B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		B3.2 Gestión de recursos humanos.	Gestión de empleados, contratistas, terceros, entre otros, incluyendo revisión de sus cualidades y capacidades así como su entrenamiento.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
				B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
				B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B3.3 Gestión de otros recursos.	Gestión operacional y de mantenimiento de recursos que tienen un impacto en el desempeño de la organización.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
				B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
				B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
				B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
				B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
				B2 Planeación.	Procesos de planeación del sistema de gestión.
				B3 Implementación y Operación.	Procesos de implementación y operación del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
				B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.
				B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
				B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
				B2.6 Planeación de procesos operacionales Previsibles.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
				B2.7 Preparación de imprevistos para los acontecimientos.	Acuerdos necesarios para manejar emergencias previsibles.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la implementación y operación exitosas del sistema de gestión.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
				B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
				B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
				B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
				B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
				B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
				B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		B5.1 Acción correctiva.	Mecanismo para la eliminación de las causas de las no conformidades en el sistema de gestión.
				B5.2 Acción preventiva.	Mecanismos para eliminar las causas potenciales de las no conformidades en el sistema de gestión.
				B5.3 Mejora continua.	Provisiones realizadas para la mejora continua del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
				B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
				B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		B3.2 Gestión de recursos humanos.	Gestión de empleados, contratistas, terceros, entre otros, incluyendo revisión de sus cualidades y capacidades así como su entrenamiento.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la implementación y operación exitosas del sistema de gestión.
Contar con una relación de las medidas de seguridad.		Art. 61		B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la implementación y operación exitosas del sistema de gestión.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 del Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
				B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
				B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		B3.5 Comunicación	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
				B2 Planeación.	Procesos de planeación del sistema de gestión.
				B3 Implementación y Operación	Procesos de implementación y operación del sistema de gestión.
				B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
				B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.
				B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
				B2 Planeación.	Procesos de planeación del sistema de gestión.
				B3 Implementación y Operación.	Procesos de implementación y operación del sistema de gestión.
				B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
				B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.
				B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	B3.1 Control Operacional	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

4.12 ISO GUIDE 73, Risk management – Vocabulary.

Introducción. El estándar proporciona las definiciones de los términos genéricos relacionados con la gestión del riesgo. El ISO Guide 73 promueve una base común de entendimiento y un enfoque coherente para la descripción de actividades y el uso uniforme de conceptos utilizados en procesos y marcos de trabajo para la gestión del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		2.1 Gestión del Riesgo.	Actividades para dirigir y controlar a una organización con respecto al riesgo.
				3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
				3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
				3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
				3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		3.8.1.1 Control.	Medida para afectar el riesgo.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		3.8.1.1 Control.	Medida para afectar el riesgo.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		3.8.1.1 Control.	Medida para afectar el riesgo.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	3.8.1.1 Control.	Medida para afectar el riesgo.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
				3.8.1.6 Riesgo Residual.	Riesgo resultante después del tratamiento de riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				3.8.2.5 Perfil de Riesgo.	Descripción de un conjunto de riesgos.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		3.3.1 Estableciendo el contexto.	Factores internos y externos para la gestión del riesgo.
				3.3.1.1 Contexto Externo.	Ambiente externo en el que la organización busca lograr sus objetivos.
				3.3.1.2 Contexto Interno.	Ambiente interno en el que la organización busca lograr sus objetivos.
				3.5.1.1 Descripción del Riesgo.	Definición estructurada del riesgo.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		2.1.2 Política de Gestión del Riesgo.	Declaración de cómo la organización gestiona el riesgo.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		NO APLICA	NO APLICA
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		3.8.2.6 Auditoría de Gestión del Riesgo.	Proceso para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
				3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
				3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.
				3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		3.8.2.6 Auditoría de Gestión del Riesgo.	Proceso para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			NO APLICA	NO APLICA
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			NO APLICA	NO APLICA
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		NO APLICA	NO APLICA
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
				3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
				3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
				3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo
				3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		NO APLICA	NO APLICA
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		NO APLICA	NO APLICA
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
				3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
				3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
				3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		3.6.1.6 Vulnerabilidad.	Susceptibilidad a una fuente de riesgo.
				3.8.1.1 Control.	Medida para afectar el riesgo.
				3.8.1.6 Riesgo Residual.	Riesgo resultante después del tratamiento de riesgo.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		2.1.3 Plan de Gestión de Riesgos.	Especifica el enfoque, componentes, y recursos para la gestión del riesgo.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		3.8.2.1 Monitoreo.	Supervisión del desempeño de la manera de gestionar el riesgo.
				3.8.2.2 Revisión.	Determinar lo adecuado y la efectividad de la gestión del riesgo.
				3.8.2.6 Auditoría de la Gestión del Riesgo.	Proceso independiente para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		NO APLICA	NO APLICA
Contar con una relación de las medidas de seguridad.		Art. 61		3.8.1.1 Control.	Medida para afectar el riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		3.3.1 Estableciendo el contexto.	Factores internos y externos para la gestión del riesgo.
				3.3.1.1 Contexto Externo.	Ambiente externo en el que la organización busca lograr sus objetivos.
				3.3.1.2 Contexto Interno.	Ambiente interno en el que la organización busca lograr sus objetivos.
				3.8.2 Términos relacionados al monitoreo y medición.	Monitoreo y medición del riesgo.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		3.8.2.1 Monitoreo.	Supervisión del desempeño de la manera de gestionar el riesgo.
				3.8.2.2 Revisión.	Determinar lo adecuado y la efectividad de la gestión del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		2.1.1 Marco de trabajo de Gestión del Riesgo.	Conjunto de componentes para el diseño, implementación, monitoreo, y seguimiento de la gestión del riesgo.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		2.1.1 Marco de trabajo de Gestión del Riesgo.	Conjunto de componentes para el diseño, implementación, monitoreo, y seguimiento de la gestión del riesgo.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		3.8.1.1 Control.	Medida para afectar el riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.13 ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.

Introducción. Es un documento de referencia para entender los términos y vocabulario relacionado con los sistemas de gestión de calidad. El ISO 9000:2005 está orientado a organizaciones que buscan tomar ventaja a través de la implementación de un sistema de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.
				0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.
				1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
				2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
				3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	2.7 Documentación	Aspectos de la documentación en los sistemas de gestión de la calidad
				2.7.1 Valor de la documentación	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las	Art. 14		Art. 15	0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
				2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
				2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
				2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles	Art. 19	Art. 9 Art. 48		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
				2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
				2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
				2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
				2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
				2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
				2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y		Art. 48 - IX		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
obligaciones que establece la Ley y su Reglamento.				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia	Art. 44			0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.				0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.
				1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
				2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
				3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
				2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
				2.3 Enfoque de sistemas de de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		2.9 Mejora continua.	Acciones encaminadas a la mejora continua del sistema de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
				2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
				2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
				2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Contar con una relación de las medidas de seguridad.		Art. 61		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de		Art. 62		2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
				2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
				2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
				2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
				2.9 Mejora continua.	Acciones encaminadas a la mejora continua del sistema de gestión de la calidad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.
				0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.
				1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
				2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
				3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
				2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
				2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.
				0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
				2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
				3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus		Art. 110	Art. 25 Art. 30	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
				2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
				2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.

4.14 BS 10012:2009 Data Protection – Specification for a Personal Information Management System (PIMS).

Introducción. Este estándar Británico ha sido producido para formar las bases para las políticas internas sobre la legislación de protección de datos y el cumplimiento con buenas prácticas y así mismo es un marco de referencia estándar para auditorías y procesos de revisión respecto a protección de datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
				4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
				5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
				6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		4.7 Procesamiento justo y lícito.	Actividades para que el procesamiento de información recopilada sea de forma licita y justa.
				4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
				4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
				4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
				4.10 Precisión.	Actividades para el mantenimiento íntegro y actualizado de los datos recopilados.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	4.8 Procesamiento de información personal para propósitos especificados.	Actividades para asegurar que la información obtenida es utilizada solo para los propósitos especificados.
				4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	4.9 Idoneidad, relevante y no excesivo.	Actividades para asegurar que la información personal es adecuada, relevante y no excesiva.
				4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
				4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
				4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
				4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
				5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
				6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
				4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
				4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
				4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
				4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
				4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
				4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
				4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
				4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
				4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		3.3 Política de gestión de información personal.	La dirección de la organización debe mantener y demostrar compromiso con una política de gestión de información personal.
				3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
				3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
				4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
				5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		3.6 Provisión de recursos.	La organización determina y provee los recursos necesarios para el mantenimiento del PIMS.
				3.7 Incrustación del Sistema de Gestión de Información Personal en la cultura de la organización.	Actividades para incluir el PIMS como un valor relevante dentro de la organización
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS
				5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
				6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
				6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
				4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
				4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
				4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
				4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
				4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
				4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
				4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
				4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.
				4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.
				4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS (Personal Information Management System).
				4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
				5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
				6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
				4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo,		Art. 59		3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
o bien, contratar a una persona física o moral para tal fin.				4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.
				4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
				4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
				4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
				4.2.1 General.	Debe ser mantenido un inventario de las categorías de información personal
				4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
				4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					información personal.
				4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
				4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
				4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
				4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
				6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
				6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
Contar con una relación de las medidas de seguridad.		Art. 61		4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
				4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
				5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
				5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
				6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
				6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
				4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
				5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
				6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a		Art. 95		4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		4.12.1 Derechos de individuos.	Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	4.12.1 Derechos de individuos.	|Establecimiento de procedimientos para la atención de los derechos de los individuos que proporcionan información personal.
				4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable:			Art. 33	4.7.1 Recolección y procesamiento de información .personal	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.				4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
				4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
				4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.

4.15 NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

Introducción. Este estándar proporciona principios y prácticas generalmente aceptadas para el aseguramiento de tecnologías de información. Los principios direccionan la seguridad desde un punto de vista de alto nivel; siendo las prácticas las que muestran lo que se debe hacer para mejorar y medir un programa de seguridad existente o en desarrollo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		2 Principios Generalmente Aceptados de Seguridad del Sistema.	Principios de seguridad utilizados como guía para el mantenimiento y desarrollo de programas de seguridad, políticas y procedimientos.
				3 Prácticas Comunes de Seguridad de TI.	Actividades mínimas a realizar para el establecimiento de un programa de seguridad.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.					
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	2 Principios Generalmente Aceptados de Seguridad del Sistema.	Principios de seguridad utilizados como guía para el mantenimiento y desarrollo de programas de seguridad, políticas y procedimientos.
				3 Prácticas Comunes de Seguridad de TI	Actividades mínimas a realizar para el establecimiento de un programa de seguridad.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
				3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		3.1 Política.	Lineamientos para el establecimiento de una política de seguridad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		3.8 Concientización y entrenamiento.	Establecimiento de un programa de concienciación y entrenamiento.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		2.3 La Seguridad en Cómputo debe ser costeable y efectiva.	Principio que indica que los costos de la seguridad no deben exceder los beneficios esperados.
				3.2 Gestión del Programa.	Actividades para la asignación de recursos y asignación de responsabilidades para el programa de seguridad.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		3.1 Política.	Lineamientos para el establecimiento de una política de seguridad.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.
				3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
				3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		3.13.1 Contenidos de los registros de auditoría.	Establece las características básicas del contenido de auditoría.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para		Art. 50		2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
				3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				3.10 Seguridad física y ambiental	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
				3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			3.4 Planeación del Ciclo de Vida.	Define las actividades para la administración del ciclo de vida del programa de seguridad.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes		Art. 52 - I		2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
				3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
				3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad		Art. 52 - II		2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
				3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.
				3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
				3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
				3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
				3.2 Gestión del Programa.	Actividades para la asignación de recursos y asignación de responsabilidades para el programa de seguridad.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados;		Art. 60		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
				3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		3.8 Concientización y entrenamiento.	Establecimiento de un programa de concienciación y entrenamiento.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.
Contar con una relación de las medidas de seguridad.		Art. 61		3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.
				3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las		Art. 65		3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.					
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		3.4 Planeación del Ciclo de Vida.	Define las actividades para la administración del ciclo de vida del programa de seguridad.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		3.4 Planeación del Ciclo de Vida.	Define las actividades para la administración del ciclo de vida del programa de seguridad.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.16 OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Introducción. Estos lineamientos establecen un marco de trabajo de los principios que aplican a todos los participantes de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la mejora de la seguridad de los sistemas de información y las redes a fin de promover la prosperidad económica y el desarrollo social.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
				2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
				3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
				4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
				6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
				9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		4. Ética.	Los participantes deben respetar los intereses legítimos de otros.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el	Art. 11	Art. 37		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
mencionado incumplimiento.					
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos		Art. 48 - II		1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
personales.					pueden hacer para mejorar la seguridad.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
				2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
				3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
				4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
				6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		5. Democracia	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Contar con una relación de las medidas de seguridad.		Art. 61		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.		Art. 62		8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.					
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
				2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
				3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
				4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
				6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
				9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
				2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
				3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
				4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
				5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
				6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
				7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
				8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.					
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.17 Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.

Introducción. Este documento desarrollado desde una perspectiva de negocio. El documento está desarrollado con base en 10 principios de privacidad, tomando como referencia la mayoría de las regulaciones locales, nacionales e internacionales. Cada uno de los principios es soportado por un objetivo medible.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		1 Gestión.	Actividades para la definición de documentación, comunicados y asignación de responsabilidades de acuerdo a las políticas y procedimientos.
				2 Aviso.	Proveer aviso sobre políticas y procedimientos de privacidad e identificar los propósitos de la recopilación de información personal.
				3 Opción y Consentimiento.	Describir las opciones sobre el consentimiento respecto a la recopilación de información personal.
				4 Recolección.	Recopilar información solo para los propósitos definidos.
				5 Uso, retención, y eliminación.	Establecimiento de los lineamientos para limitar el uso, retención y eliminación de información personal.
				6 Acceso.	Proveer al titular acceso para la revisión y actualización de sus datos.
				7 Divulgación a terceros.	Delimita la transmisión de información a terceros solo para los propósitos establecidos.
				8 Seguridad para Privacidad.	Actividades para la protección de datos personales contra accesos no autorizados.
				9 Calidad.	La entidad mantiene la información completa, actualizada y actual.
				10 Monitoreo y cumplimiento.	Actividades para asegurar el cumplimiento de las políticas de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		4.1.0 Política de Privacidad.	Alineación de políticas de privacidad a la colección de información personal.
				4.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				4.1.2 Tipos de información personal recopilada y métodos de recopilación.	Métodos para la recolección de información y tipos de información de acuerdo al aviso de privacidad.
				4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
				4.2.2 Recolección por medios justos y legales.	Métodos para la recolección de información revisados por la dirección.
				4.2.3 Recolección mediante terceros.	La dirección confirma que los terceros de donde recopila información son seguros y legales.
				4.2.4 Información desarrollada sobre individuos.	Procedimientos por el cual se informa al titular si se adquiere información personal.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		3.1.0 Política de Privacidad.	Definición de la política de privacidad.
				3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
				3.1.2 Consecuencias de negar o retirar el consentimiento.	Informar al titular sobre las consecuencias de negar a proporcionar información personal, negar o retirar el consentimiento.
				3.2.1 Consentimiento implícito o explícito.	Obtención del consentimiento en el momento o antes de la recopilación de datos personales.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	3.1.0 Política de Privacidad.	Definición de la política de privacidad incluyendo opciones y consentimiento.
				3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
				3.1.2 Consecuencias de negar o retirar el consentimiento.	Informar al titular sobre las consecuencias de negar a proporcionar información personal, negar o retirar el consentimiento.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		3.1.0 Política de Privacidad.	Definición de la política de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
				3.2.1 Consentimiento implícito o explícito.	Obtención del consentimiento en el momento o antes de la recopilación de datos personales.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	3.2.3 Consentimiento explícito para información sensible.	Obtención de consentimiento explícito siempre que se recopile información sensible.
				4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
				5.2.1 Uso de información personal.	Indica que la información personal es utilizada solo para los propósitos establecidos después de la obtención del consentimiento del titular.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
				9.2.1 Exactitud de información personal.	La información recopilada debe ser exacta y completa.
				9.2.2 Relevancia de información personal.	La información personal debe ser relevante a los propósitos establecidos
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las	Art. 11	Art. 37		5.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.				5.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				5.2.1 Uso de información personal.	La información personal recopilada solo puede ser utilizada para los propósitos definidos.
				5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
				5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		5.2.1 Uso de información personal.	La información personal recopilada solo puede ser utilizada para los propósitos definidos.
				5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
				5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
				5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso,

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					retención y eliminación de su información personal.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
				4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
			Art. 36 Art. 38	2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
				4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				4.2.3 Recolección mediante terceros.	La dirección confirma que los terceros de donde recopila información son seguros y legales.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
				2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
				8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
				8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.2.4 Salvaguardas Ambientales.	Establecimiento de controles ambientales para la protección de información personal.
				8.2.5 Información personal transmitida.	Controles para la transmisión segura de datos personales.
				8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
				8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		1.1.1 Comunicación a personal interno.	Políticas, procedimientos Sanciones relacionadas a privacidad deben ser comunicadas al personal interno.
				1.1.2 Responsabilidad y rendición de cuentas de las Políticas.	Asignación de roles y responsabilidades sobre privacidad deben ser establecidas y comunicadas.
				1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
				1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones relacionadas relevantes.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
				1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
				1.2.8 Recursos de soporte.	Recursos suficientes para la implementación de las políticas de privacidad.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				1.2.6 Gestión de infraestructura y sistemas.	Procesos para la administración y control de la infraestructura que soporta el almacenamiento y procesamiento de información personal.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
				1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.
				1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones
				8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		10.2.1 Proceso de atención de dudas, quejas y disputas.	Procedimiento para la atención de quejas y disputas
				10.2.2 Resolución de disputas.	Base de conocimiento sobre la resolución de quejas y disputas.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		1.1.1 Comunicación a personal interno.	Políticas, procedimientos Sanciones relacionadas a privacidad deben ser comunicadas al personal interno.
				1.1.2 Responsabilidad y rendición de cuentas de las Políticas.	Asignación de roles y responsabilidades sobre privacidad deben ser establecidas y comunicadas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
				8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
				8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.
				8.2.4 Salvaguardas Ambientales.	Establecimiento de controles ambientales para la protección de información personal.
				8.2.5 Información personal transmitida.	Controles para la transmisión segura de datos personales.
				8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
				8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
				8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.
				8.2.5 Información personal transmitida.	Controles para la transmisión segura de datos personales.
				8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50		1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
				7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
				6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.
				2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
				7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de	Art. 44			1 Gestión.	Actividades para la definición de documentación, comunicados y asignación de responsabilidades de acuerdo a las políticas y procedimientos.
				2 Aviso.	Proveer aviso sobre políticas y procedimientos de privacidad e identificar los propósitos de la recopilación de información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
incumplimiento.				3 Opción y Consentimiento.	Describir las opciones sobre el consentimiento respecto a la recopilación de información personal.
				4 Recolección.	Recopilar información solo para los propósitos definidos.
				5 Uso, retención, y eliminación.	Establecimiento de los lineamientos para limitar el uso, retención y eliminación de información personal.
				6 Acceso.	Proveer al titular acceso para la revisión y actualización de sus datos.
				7 Divulgación a terceros.	Delimita la transmisión de información a terceros solo para los propósitos establecidos.
				8 Seguridad para Privacidad.	Actividades para la protección de datos personales contra accesos no autorizados.
				9 Calidad.	La entidad mantiene la información completa, actualizada y actual.
				10 Monitoreo y cumplimiento.	Actividades para asegurar el cumplimiento de las políticas de privacidad.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
				1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
				7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación,		Art. 52 - II		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
				1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
				4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
				5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
				7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta		Art. 54		1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.				7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		1.2.3 Identificación y clasificación de información personal.	Inventario de información personal y datos sensibles.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
				1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones relacionadas relevantes.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas		Art. 61 - IV		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
implementadas de manera efectiva.				8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
				8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
				10.2.3 Revisión de cumplimiento.	El cumplimiento con las leyes y regulaciones vigentes, contratos y
				10.2.4 Instancias de no cumplimiento.	El incumplimiento con leyes regulaciones o contratos deben ser documentadas y corregidas.
				10.2.5 Monitoreo continuo.	Procedimientos para el monitoreo periódico de la efectividad del sistema
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
				1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones relacionadas relevantes.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
Contar con una relación de las medidas de seguridad.		Art. 61		8.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				8.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				8.2.1 Programa de Seguridad de la Información.	8.2.1 Programa de Seguridad de la Información.
				8.2.2 Controles de Acceso Lógico.	8.2.2 Controles de Acceso Lógico.
				8.2.3 Controles de Acceso Físico.	8.2.3 Controles de Acceso Físico.
				8.2.4 Salvaguardas Ambientales.	8.2.4 Salvaguardas Ambientales.
				8.2.5 Información personal transmitida.	8.2.5 Información personal transmitida.
				8.2.6 Información personal en medios móviles.	8.2.6 Información personal en medios móviles.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
				1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.
				1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
				1.2.6 Gestión de infraestructura y sistemas.	Procesos para la administración y control de la infraestructura que soporta el almacenamiento y procesamiento de información personal.
				1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus		Art. 65		1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.					
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de		Art. 70		7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
				7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
				7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
				7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
				7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer		Art. 90	Art. 28	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
				2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
				6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				6.2.2 Confirmación de la identidad del individuo.	El titular que solicita acceso a sus datos debe confirmar su identidad.
				6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
				6.2.4 Negación de acceso.	Procedimiento para la ejecución del derecho de acceso.
				6.2.5 Actualización o corrección de información personal.	Procedimiento para que el titular corrija o actualice su información personal.
				6.2.6 Manifestación de desacuerdo.	Procedimiento para que el titular corrija o actualice su información personal.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la		Art. 95		6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
correspondiente fecha de recepción.				6.2.2 Confirmación de la identidad del individuo.	El titular que solicita acceso a sus datos debe confirmar su identidad.
				6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
				6.2.4 Negación de acceso.	Procedimiento para la ejecución del derecho de acceso.
				6.2.5 Actualización o corrección de información personal.	Procedimiento para que el titular corrija o actualice su información personal.
				6.2.6 Manifestación de desacuerdo.	Procedimiento para que el titular corrija o actualice su información personal.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				6.2.2 Confirmación de la identidad del individuo.	El titular que solicita acceso a sus datos debe confirmar su identidad.
				6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
				6.2.4 Negación de acceso.	Procedimiento para la ejecución del derecho de acceso.
				6.2.5 Actualización o corrección de información personal.	Procedimiento para que el titular corrija o actualice su información personal.
				6.2.6 Manifestación de desacuerdo.	Procedimiento para que el titular corrija o actualice su información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				6.2.2 Confirmación de la identidad del individuo.	El titular que solicita acceso a sus datos debe confirmar su identidad.
				6.2.3 Información personal entendible, tiempo, y costo.	El acceso a la información por parte del individuo, debe ser de manera clara y a un costo razonable.
				6.2.4 Negación de acceso.	Procedimiento para la ejecución del derecho de acceso.
				6.2.5 Actualización o corrección de información personal.	Procedimiento para que el titular corrija o actualice su información personal.
				6.2.6 Manifestación de desacuerdo.	Procedimiento para que el titular corrija o actualice su información personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
				2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
				2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos
				2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuales son los procesos y actividades cubiertas por dichas políticas y procedimientos.
				2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
				3.2.2 Consentimiento para nuevos propósitos o usos.	Obtener consentimiento para procesar información personal bajo nuevos propósitos.

4.18 Control Objectives for Information and Related Technology (COBIT v4.1).

Introducción. COBIT 4.1 es un marco de referencia que sirve como guía para la implementación del gobierno y gestión de los recursos de TI en las organizaciones. El objetivo de este marco de referencia el proporcional valor a la organización por medio de un coste óptimo de recursos mientras los riesgos también son controlados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		PO2 Definir la Arquitectura de la Información.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
				PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				AI6 Administrar cambios.	Definición de políticas y procedimientos para la administración de cambios.
				AI7 Instalar y acreditar soluciones y cambios.	Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación
				DS4 Garantizar la continuidad del servicio.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio
				DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		PO2.1 Modelo de Arquitectura de Información Empresarial.	Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI.
				PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos.	Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización.
				PO2.4 Administración de Integridad.	Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico.
				PO8.3 Estándares de Desarrollo y de Adquisición.	Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados.
				DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
				DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
				DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	PO2 Definir la Arquitectura de la Información.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
				PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				AI6 Administrar cambios.	Definición de políticas y procedimientos para la administración de cambios.
				AI7 Instalar y acreditar soluciones y cambios.	Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación.
				DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
				DS4 Garantizar la continuidad del servicio.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
				DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales
				AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		PO6.1 Ambiente de Políticas y de Control.	Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.
				PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI.	Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y el control que se alinee con la política de TI, el ambiente de control y el marco de trabajo de riesgo y control de la empresa.
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		PO7.4 Entrenamiento del Personal de TI.	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar y mejorar su conocimiento.
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
				DS7 Educar y Entrenar a los Usuarios.	Educar y entrenar a los usuarios respecto a los servicios de TI ofrecidos.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
				DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado en la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
				AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					de los requerimientos.
				DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
				DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		DS8.1 Mesa de Servicios.	Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados,

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					requerimientos de servicio y solicitudes de información.
				DS8.2 Registro de Consultas de Clientes.	Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.
				DS8.3 Escalamiento de Incidentes.	Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas.
				DS8.4 Cierre de Incidentes.	Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
				DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
				DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				PO3.4 Estándares Tecnológicos.	Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas.
				PO4.9 Propiedad de los datos y sistemas.	Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.
				AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
				DS12.3 Acceso Físico.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		AI2.3 Control y Posibilidad de Auditar las Aplicaciones.	Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.
				DS5.3 Administración de Identidad.	Asegurar que todos los usuarios y su actividad en sistemas de TI deben ser identificables de manera única.
				DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
				DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados.		Art. 50		PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
				PO4.15 Relaciones.	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI.
				AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
				PO4.15 Relaciones.	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI.
				DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.3 Sistema de Administración de Librerías de Medios.	Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.
				DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento.	Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			DS8.4 Cierre de Incidentes.	Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		PO7.6 Procedimientos de Investigación del Personal.	Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI.
				DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes		Art. 52 - I		PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
				AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio
				DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se		Art. 52 - II		PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
				AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.
				DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
				DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento.	Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
				AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
				AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos
				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
				DS9 Administrar la configuración.	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS11.3 Sistema de Administración de Librerías de Medios.	Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.
				DS13.4 Documentos Sensitivos y Dispositivos de Salida.	Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		PO4.9 Propiedad de los datos y sistemas.	Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
				AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos.
				AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS5.3 Administración de Identidad.	Asegurar que todos los usuarios y su actividad en sistemas de TI deben ser identificables de manera única.
				DS5.4 Administración de Cuentas del Usuario.	Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados estén controlados por medio de políticas y procedimientos.
				DS5.7 Protección de la Tecnología de Seguridad.	Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.
				DS5.8 Administración de Llaves Criptográficas.	Determinar las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas
				DS5.9 Prevención, Detección y Corrección de Software Malicioso.	Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware.
				DS5.10 Seguridad de la Red.	Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
				DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
				DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		PO7.4 Entrenamiento del Personal de TI.	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar y mejorar su conocimiento,
				DS7 Educar y Entrenar a los Usuarios.	Educar y entrenar a los usuarios respecto a los servicios de TI ofrecidos.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		DS9 Administrar la configuración.	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS11.3 Sistema de Administración de Librerías de Medios.	Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.
Contar con una relación de las medidas de seguridad.		Art. 61		AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos
				AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
				PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales
				AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
				AI3.3 Mantenimiento de la Infraestructura.	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					administración de cambios de la organización.
				DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
				DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
				DS10.2 Rastreo y Resolución de Problemas.	El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
				DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
				DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
				ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	DS8.1 Mesa de Servicios.	Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.
				DS8.2 Registro de Consultas de Clientes.	Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		DS8 Administrar la Mesa de Servicio y los Incidentes.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		DS8.1 Mesa de Servicios.	Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.
				DS8.2 Registro de Consultas de Clientes.	Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		DS8 Administrar la Mesa de Servicio y los Incidentes.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		DS8 Administrar la Mesa de Servicio y los Incidentes.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
				DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	DS8.2 Registro de Consultas de Clientes.	Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

4.19 Control Objectives for Information and Related Technology (COBIT 5).

Introducción. COBIT 5 es un marco de referencia que sirve como guía para la implementación del gobierno y gestión de los recursos de Tecnología de Información en la organizaciones. El objetivo de este marco de referencia es proporcionar valor a la organización por medio de un costo óptimo de recursos mientras los riesgos también son controlados. COBIT 5 toma en cuenta las versiones anteriores, y añade mejoras en procesos, prácticas, actividades, métricas, y modelos de madurez principalmente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
				APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
				BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
				DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
				APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC
				APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	Criterios para incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollo de soluciones y los servicios ofrecidos.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
				DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
				DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
Al responsable le corresponde demostrar que los		Art. 39		APO03.02 Definir la arquitectura de	La arquitectura de referencia describe la

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.				referencia.	situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
				DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el	Art. 12	Art. 23	Art. 6 Art. 8	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
aviso de privacidad.				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
				APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
				BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
				DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
Los responsables no adoptarán medidas de	Art. 19	Art. 9		APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.		Art. 48			en todos los procesos de la organización.
				APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		EDM03.02 Orientar la gestión de riesgos.	Orientar el establecimiento de prácticas de gestión de riesgos a asegurar que no se exceda el apetito del riesgo.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				APO01.03 Mantener los elementos catalizadores del sistema de gestión.	Actividades para el mantenimiento de elementos catalizadores dentro de los objetivos de la organización.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
				APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades dentro de la organización.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
				DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos		Art. 48 - VII		DSS02.01 Definir esquemas de clasificación de incidentes y	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
personales.				peticiones de servicio.	
				DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	Procedimientos para el registro y gestión de incidentes.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
				DSS02.04 Investigar, diagnosticar y localizar incidentes.	Procedimientos para el diagnóstico, investigación y localización de incidentes de seguridad.
				DSS02.05 Resolver y recuperarse de incidentes.	Procedimientos para la resolución y recuperación de servicios afectados por incidentes de seguridad.
				DSS02.06 Cerrar peticiones de servicio e incidentes.	Criterios para el cierre de incidentes y solicitudes de servicio.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
				DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
				DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				APO03.05 Proveer los servicios de arquitectura empresarial.	Guías de los proyectos, formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura.
				APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
				BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
				BAI03.02 Diseñar los componentes	Criterios para la elaboración de diseños

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				detallados de la solución.	progresivos considerando todos los componentes.
				BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
				BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
				APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
				DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.		Art. 50		APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
				APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
				APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
				DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			DSS02.05 Resolver y recuperarse de incidentes.	Procedimientos para la resolución y recuperación de servicios afectados por incidentes de seguridad.
				DSS02.06 Cerrar peticiones de servicio e incidentes.	Criterios para el cierre de incidentes y solicitudes de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		APO07.01 Mantener la dotación de personal suficiente y adecuado.	Criterios para mantener solo a personal necesario de acuerdo a las necesidades del negocio.
				APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes		Art. 52 - I		APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
				APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.	Criterios para la identificación y categorización de proveedores.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;		Art. 52 - II		APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
				APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.	Criterios para la identificación y categorización de proveedores.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
				APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance		Art. 54		APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares.		Art. 60		APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
				BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
				BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
				BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
				APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
				BAI10 Gestionar la Configuración.	Definir y mantener registros y relaciones entre los principales recursos y capacidades necesarios para la prestación de servicios.
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
				BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
				BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
				BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio,

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					seguridad y auditabilidad.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.01 Proteger contra software malicioso (malware).	Actividades de control contra software malicioso.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
				APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
				DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades dentro de la organización.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		BAI10 Gestionar la Configuración	Definir y mantener registros y relaciones entre los principales recursos y capacidades necesarios para la prestación de servicios.
				DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
Contar con una relación de las medidas de seguridad.		Art. 61		BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
				BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
				BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					(QA) y estándares de aprobación.
				BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.		Art. 62		APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
				APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
				BAI03.10 Mantener soluciones.	Criterios para desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
IV. Exista una afectación a los datos personales distinta a las anteriores.				DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para		Art. 66		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.				DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
				DSS03.02 Investigar y diagnosticar problemas.	Criterios para el proceso de investigación y diagnostico de problemas.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
				APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
				DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
				MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
				DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	Procedimientos para el registro y gestión de incidentes.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		DSS02 Gestionar las Peticiones y los Incidentes del Servicio	Criterios para el registro, seguimiento, asignación, resolución y cierre de las solicitudes e incidentes del servicio.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		DSS02 Gestionar las Peticiones y los Incidentes del Servicio.	Criterios para el registro, seguimiento, asignación, resolución y cierre de las solicitudes e incidentes del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		DSS02 Gestionar las Peticiones y los Incidentes del Servicio.	Criterios para el registro, seguimiento, asignación, resolución y cierre de las solicitudes e incidentes del servicio.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		DSS02 Gestionar las Peticiones y los Incidentes del Servicio.	Criterios para el registro, seguimiento, asignación, resolución y cierre de las solicitudes e incidentes del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
				DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
				DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
				DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
				DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
				DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	Procedimientos para el registro y gestión de incidentes.
				DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
				DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
				DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
				DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
				DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.

4.20 PCI DSS, Payment Card Industry Data Security Standard v2.0.

Introducción. Este estándar fue desarrollado por un comité conformado por las compañías de tarjetas bancaria más importantes, como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, a asegurar dichos datos con el fin de prevenir los fraudes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
				Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
				Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
				Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
				Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	3.2 No almacene datos confidenciales de autenticación después de recibir la autorización.	Guías para el borrado seguro de datos confidenciales del tarjetahabiente cuando ya no son necesarios.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		NO APLICA	NO APLICA
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
				Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
				Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
				Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
				Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.
				Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
				Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
				Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
				Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
				Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
				Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
				Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
				Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
				Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
				Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		12.1 Establezca, publique, mantenga y distribuya una política de seguridad.	Guías para la definición y comunicación de la política de seguridad.
				12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
				12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.
				12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Implementación del programa de concienciación de seguridad de la información.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
				12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.
				12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y		Art. 48 - IX		Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
obligaciones que establece la Ley y su Reglamento.				Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
				Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
				Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
				Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
				Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
				Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
				Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
				Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
				Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
				Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		10.2 Implemente pistas de auditoría automatizadas para todos los componentes del sistema.	Guías para la verificación de pistas de auditoría en los sistemas y aplicaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.	Guías para el resguardo de las pistas de auditoría.
				10.6 Revise los registros de todos los componentes del sistema al menos una vez al día.	Guías para el monitoreo de los componentes de los sistemas.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
				12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo.	Guías para la asignación de un responsable de la seguridad de la información en la organización.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
				Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
				Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
				Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
				Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
				12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
				12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
				12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.
				Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
				12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
				12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
				12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
				Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo.	Guías para la asignación de un responsable de la seguridad de la información en la organización.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		9.7.1 Clasifique los medios de manera que se pueda determinar la confidencialidad de los datos.	Guías para la clasificación de los datos.
				9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
				9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.
				Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
				Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
				Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
				Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
				Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
				Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
				Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
				Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
				Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
				Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
				12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
				12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		9.7.1 Clasifique los medios de manera que se pueda determinar la confidencialidad de los datos.	Guías para la clasificación de los datos.
				9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
				9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.
				Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
				Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
				Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
				Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
				Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
				Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
				Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
				Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
				Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
				Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
				Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
				12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
				12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
				Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
				Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
				Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
				Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
				Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
				Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
				Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
				Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
				Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.21 HIPAA, Health Insurance Portability and Accountability Act.

Introducción. HIPAA es una ley federal americana que se conoce como Ley de Portabilidad y Responsabilidad del Seguro Médico y su objetivo fundamental es el de facilitar a las personas el mantener un seguro médico, proteger la confidencialidad y la seguridad de la información del cuidado médico y ayudar a la industria del cuidado de la salud a controlar los costos administrativos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		164.502 Usos y revelaciones de información protegida de salud: Reglas generales.	Disposiciones para usos y revelaciones solamente autorizados con respecto a la información de salud.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
				164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
				164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
				164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
				164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		164.312(b) Controles de auditoría.	Mecanismos para registrar y examinar los sistemas que contienen información de salud.
				164.312(c)(1) Integridad.	Políticas y procedimientos para proteger la integridad información electrónica de salud.
				164.312(e)(1) Seguridad en la transmisión.	Medidas técnicas para la protección de la información de salud transmitida por la red.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
				164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
				164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
				164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
				164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
				164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
				164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
				164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
				164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			164.308(a)(7)(ii)(A) Plan de respaldo de datos.	Procedimientos para el respaldo de datos de salud.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			164.308(a)(2) Asignación de la responsabilidad de seguridad.	Asignación de oficial de seguridad responsable del desarrollo e implementación de políticas y procedimientos de seguridad.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
				164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
				164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
				164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
				164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		164.308(a)(2) Asignación de la responsabilidad de seguridad.	Asignación de oficial de seguridad responsable del desarrollo e implementación de políticas y procedimientos de seguridad.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
				164.308(a)(1)(ii)(D) Revisión de la actividad del sistema de información.	Procedimientos para la revisión de registros de sistemas de información que contienen información de salud.
				164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
				164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		164.308(a)(3)(ii)(A) Autorización y/o supervisión.	Procedimientos para la autorización y/o supervisión de empleados que acceden a información de salud.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
				164.316(b)(2)(iii) Actualizaciones.	Actualización periódica de la documentación ante cambios que afectan la seguridad de la información de salud.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
				164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
Contar con una relación de las medidas de seguridad.		Art. 61		164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
				164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
				164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
				164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
				164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
				164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
				164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
				164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
				164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
				164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.308(b)(4) Contrato escrito.	Disposiciones para que las personas requieran la corrección de su información de salud.
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
				164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

4.22 SOx, Sarbanes-Oxley Act of 2002.

Introducción. La Ley SOx nace en Estados Unidos con el fin de supervisar a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversionista.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	Esta sección establece las responsabilidades corporativas de las empresas emisoras con respecto a los reportes financieros de resultados.
				Sección 404. Evaluación Gerencial de los Controles Internos.	Esta sección establece las obligaciones y responsabilidades de las empresas emisoras en la evaluación de sus controles internos con respecto a los reportes financieros de resultados.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		NO APLICA	NO APLICA
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		NO APLICA	NO APLICA
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		NO APLICA	NO APLICA
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de	Art. 19	Art. 47		Sección 404. Evaluación Gerencial de los Controles Internos.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.		Art. 57		(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
				(a) Reglamentos requeridos.	
				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
				(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		NO APLICA	NO APLICA
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		NO APLICA	NO APLICA
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(b) Evaluación y reporte del Control Interno. Con respecto a la evaluación del control interno requerido, cada despacho contable que prepare o emita un reporte de auditoría para el emisor atestiguara, y reportará sobre la evaluación realizada por la Gerencia del emisor. Un atestiguamiento debe ser realizado de acuerdo con estándares para proyectos de atestiguamiento emitidos o adoptados por la PCAOB.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Dicho atestiguamiento no será sujeto de un proyecto separado.	
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
				(a) Reglamentos requeridos.	
				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
				(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(2) Contener una evaluación, a partir del más reciente año fiscal del emisor, de la efectividad de la estructura de control interno y los procedimientos del emisor para el reporte financiero.	
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas. (1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		NO APLICA	NO APLICA
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		NO APLICA	NO APLICA
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			NO APLICA	NO APLICA
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			NO APLICA	NO APLICA
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad de los datos personales sobre los que se preste el servicio.		Art. 52 - I		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		NO APLICA	NO APLICA
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		NO APLICA	NO APLICA
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas. (1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
				(a) Reglamentos requeridos.	
				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
				(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		NO APLICA	NO APLICA
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
				(a) Reglamentos requeridos.	
				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
				(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(2) Contener una evaluación, a partir del más reciente año fiscal del emisor, de la efectividad de la estructura de control interno y los procedimientos del emisor para el reporte financiero.	
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		NO APLICA	NO APLICA
Contar con una relación de las medidas de seguridad.		Art. 61		Sección 404. Evaluación Gerencial de los Controles Internos.	
				(a) Reglas requeridas.	
				(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
				(a) Reglamentos requeridos.	
				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
				(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		NO APLICA	NO APLICA
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		NO APLICA	NO APLICA
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		NO APLICA	NO APLICA
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.23 ITIL, Information Technology Infrastructure Library v3.

Introducción. Conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de tecnología de información. Su propósito fundamental es servir como guía que abarque toda infraestructura, desarrollo y operaciones de tecnología de información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Estrategia del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.
				Diseño del Servicio.	Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.
				Transición del Servicio.	Procesos requeridos para colocar un servicio de TI de manera operacional.
				Operación del Servicio.	Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.
				Mejora continua del Servicio.	Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD3.6.3 Diseño de la arquitectura tecnológica.	Prácticas para el diseño de la arquitectura tecnológica que cubra las necesidades presentes y futuras del negocio.
				SD3.9 Arquitectura orientada al servicio.	Prácticas para que los procesos y soluciones de negocio cuenten con un enfoque de arquitectura orientada al servicio.
				SD3.10 Gestión de servicio al negocio.	Prácticas para que los componentes de TI se encuentren ligados a los objetivos y metas del negocio.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				ST4.7 Gestión del conocimiento.	Prácticas recomendadas para la gestión del conocimiento necesario para la toma de decisiones.
				SD7 Consideraciones tecnológicas.	Recomendaciones para el uso de herramientas y técnicas en el diseño de servicios.
				SS6.5 Estrategia de sourcing.	Recomendaciones para definir la estrategia de outsourcing.
				SD3.5 Actividades de diseño.	Procesos principales para el diseño de servicios de TI.
				SD3.11 Modelos para el diseño de los servicios.	Consideraciones para la adopción de un modelo para el diseño de los servicios.
				SD5.3 Gestión de aplicaciones.	Prácticas para la gestión efectiva de aplicaciones.
				ST3.2.3 Adopción de estándares y de un marco de trabajo común.	Lineamientos para adoptar un estándar y un marco de trabajo común para la transición de servicios de TI.
				ST4.1.5.1 Estrategia de transición.	Recomendaciones para la adopción de una estrategia de transición de servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
				SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
				SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las	Art. 14		Art. 15	Estrategia del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				Diseño del Servicio.	Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.
				Transición del Servicio.	Procesos requeridos para colocar un servicio de TI de manera operacional.
				Operación del Servicio.	Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.
				Mejora continua del Servicio.	Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y	Art. 19	Art. 47 Art. 57		SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.				SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				Apéndice E Detalles de la gestión de las instalaciones.	Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		SS7.5 Estrategia y mejora.	Aspectos de calidad al cliente a considerar en la definición de la estrategia del servicio de TI.
				SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
				SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
				SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				Apéndice E Detalles de la gestión de las instalaciones.	Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		SS6.4 Cultura organizacional.	Aspectos para incrementar la efectividad organizacional.
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
				CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
				CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
				SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
				SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
				SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
				SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
				CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
				SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				ST3.2.13 Asegurar la calidad de un servicio nuevo o modificado.	Principios y mejores prácticas para lograr la calidad de un servicio nuevo o modificado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
				SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
				SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata	Art. 20	Art 63 Art. 64		SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
				SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
				SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
				SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar	Art. 21	Art. 9		SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
sus relaciones con el titular o, en su caso, con el responsable.				SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
				SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			SD6.4 Roles y responsabilidades.	Roles y responsabilidades para el diseño de servicios de TI.
				SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			SO4.1.5.10 Cerrar eventos.	Actividades a considerar para el cierre de eventos en los servicios de TI.
				SO4.2.5.9 Cierre de incidentes.	Actividades a considerar para el cierre de incidentes en los servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
				SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
				SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
				SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
				SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
				SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
				SD4.6 Gestión de la seguridad de la información.	Prácticas para la gestión de proveedores.
				SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.12 Gestión del centro de datos e instalaciones.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		SD6.4 Roles y responsabilidades.	Roles y responsabilidades para el diseño de servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
				SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
				SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
				SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
				SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
				SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
				SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				ST4.3.5.3 Identificación de la configuración.	Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.
				SO5.2.4 Datos electrónicos e impresos.	Prácticas para el manejo de datos en formato electrónico e impreso.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		SO6.3 Gestión técnica.	Roles y responsabilidades para la gestión de la infraestructura de TI.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
				SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
				SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
				SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
				SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
				SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
				SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		NO APLICA	NO APLICA
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		NO APLICA	NO APLICA
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
				CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
				CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
				SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		ST4.3.5.3 Identificación de la configuración.	Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
				SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
				SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
				SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
				SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
				CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
				CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
				SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
				SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
				SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
				SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
				SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
				SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
				SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.
				SO5.7 Administración de bases de datos.	Prácticas recomendadas para la gestión de bases de datos.
				SO5.8 Gestión de servicios de directorio.	Prácticas recomendadas para la gestión de servicios de directorio.
				SO5.9 Soporte de estaciones de trabajo.	Actividades a considerar para el soporte de la operación de estaciones de trabajo.
				SO5.10 Gestión de middleware.	Prácticas recomendadas para la gestión de los componentes middleware de los servicios de TI.
				SO5.11 Gestión Internet/web.	Prácticas recomendadas para la gestión de servicios basados en web.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				SD4.6 Gestión de la seguridad de la información	Prácticas recomendadas para la gestión de la seguridad de la información.
				SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
				SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
				SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
				SO4.4 Gestión de problemas.	Prácticas para la gestión de problemas presentados en la operación de los servicios de TI.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el		Art. 69		SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
responsable que transfiere y en el receptor de los datos personales.					
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
				SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
				SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
				SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		SS7.5 Estrategia y mejora.	Aspectos de calidad al cliente a considerar en la definición de la estrategia del servicio de TI.
				SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes.		Art. 90	Art. 28	SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de		Art. 98		SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
conformidad con los plazos establecidos en el artículo 32 de la Ley.				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
				SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
				SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
				SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
				SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.

4.24 The Open Web Application Security Project (OWASP), Guía de Documentación v2.0.

Introducción. OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La guía OWASP provee lineamientos detallados sobre la seguridad de las aplicaciones web.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
					contra intérpretes comunes.
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		NO APLICA	NO APLICA
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	NO APLICA	NO APLICA
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos.	Art. 11	Art. 37		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		NO APLICA	NO APLICA
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		NO APLICA	NO APLICA
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	NO APLICA	NO APLICA
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado	Art. 14		Art. 15	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
				Pilares esenciales de la seguridad de la información.	Consideraciones de la integridad, disponibilidad, y confidencialidad de la información para la producción de un control robusto de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
en todo momento por él o por terceros con los que guarde alguna relación jurídica.				Arquitectura de seguridad.	Integración de los pilares de integridad, disponibilidad, y confidencialidad de la información en el desarrollo de aplicaciones.
				Principios de seguridad.	Lineamientos fundamentales para el desarrollo seguro de aplicaciones.
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	NO APLICA	NO APLICA
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	NO APLICA	NO APLICA
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 47 Art. 57		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		Educación del usuario.	Consideraciones para entrenar a los usuarios con respecto a la seguridad de la información.
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		NO APLICA	NO APLICA
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		NO APLICA	NO APLICA
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		NO APLICA	NO APLICA
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		NO APLICA	NO APLICA
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y		Art. 48 - IX		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
obligaciones que establece la Ley y su Reglamento.				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X		Manejo de errores, auditoría, y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
				Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		NO APLICA	NO APLICA
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			Seguridad en base de datos.	Guías para el almacenamiento seguro de la información del usuario.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			NO APLICA	NO APLICA
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			NO APLICA	NO APLICA
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		NO APLICA	NO APLICA
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante		Art. 52 - II		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último.		Art. 54		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.					
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.		Art. 59		Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
				Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
				Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
				Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
				Phishing.	Guías para la prevención del phishing.
				Servicios web.	Guías para el aseguramiento de servicios web.
				Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
				Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
				Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
				Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
				Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
				Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
				Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
				Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
				Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
				Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
				Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
				Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
				Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		NO APLICA	NO APLICA
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI		NO APLICA	NO APLICA
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		NO APLICA	NO APLICA
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		NO APLICA	NO APLICA
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.
Contar con una relación de las medidas de seguridad.		Art. 61		NO APLICA	NO APLICA
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
				Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
				Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		NO APLICA	NO APLICA
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		NO APLICA	NO APLICA
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		NO APLICA	NO APLICA
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	NO APLICA	NO APLICA
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		NO APLICA	NO APLICA
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		Seguridad en base de datos.	Guías para el almacenamiento seguro de la información del usuario.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

4.25 Cloud Security Alliance Cloud Controls Matrix (CCM) v3.0.

Introducción. Esta matriz está diseñada para proporcionar principios de seguridad para evaluar el riesgo de seguridad de un proveedor de cómputo en la nube. El documento contiene un marco de trabajo de controles que se encuentran divididos en 13 dominios.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9		Seguridad de la Aplicación y de Interfaz.	Conjunto de controles destinados a brindar seguridad a las aplicaciones y sus interfaces con otros sistemas.
				Aseguramiento de Auditoría y Cumplimiento.	Conjunto de controles para llevar a cabo la auditoría y revisión del cumplimiento de infraestructura de TI y de aplicaciones.
				Gestión de la Continuidad del Negocio y Capacidad de Recuperación Operacional.	Conjunto de controles para brindar continuidad del negocio y recuperación de los procesos que dependen de TI.
				Control de Cambios y Gestión de la Configuración.	Conjunto de controles para controlar cambios al ambiente operativo y gestionar la configuración de infraestructura de TI y aplicaciones.
				Seguridad de Datos y Gestión del Ciclo de Vida de la Información.	Conjunto de controles para brindar la seguridad de los datos y de la información durante su ciclo de vida.
				Seguridad del Centro de Datos.	Conjunto de controles físicos para la seguridad en los centros de datos.
				Gestión de Cifrado y Llaves.	Conjunto de controles para implementar cifrado de la información y gestión de las llaves de cifrado.
				Gobierno y Gestión de Riesgo.	Controles y actividades para gestión de riesgos de seguridad, y de cumplimiento regulatorio.
				Recursos Humanos.	Controles y prácticas para contar con seguridad en las relaciones con los empleados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Gestión de Identidades y Accesos.	Controles para la gestión de identidades de los usuarios y procesos, y el control de acceso a la infraestructura de TI y aplicaciones.
				Infraestructura y Seguridad en la Virtualización.	Controles para dar seguridad en ambientes virtualizados.
				Interoperabilidad y Portabilidad.	Controles y prácticas para brindar interoperabilidad y portabilidad a las aplicaciones que funcionan en un esquema de cómputo en la nube.
				Seguridad Móvil.	Controles y prácticas para la seguridad por el uso de dispositivos móviles.
				Gestión de Incidentes de Seguridad, Forense en la Nube, y Descubrimiento Electrónico.	Controles y prácticas para la detección y atención de incidentes de seguridad.
				Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.	Gestión de terceros que participan como proveedores para brindar los servicios de cómputo en la nube a los clientes finales.
				Gestión de Amenazas y Vulnerabilidades.	Controles y prácticas para el manejo adecuado de amenazas y vulnerabilidades de seguridad informática.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los datos personales deberán recabarse y tratarse de manera lícita. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 10 Art. 44		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán el consentimiento explícito de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11		NO APLICA	NO APLICA
Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.	Art. 8	Art. 21	Art. 29	NO APLICA	NO APLICA
Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 15 Art. 56	Art. 23	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	Art. 11	Art. 36		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				CCC-03 Prueba de Calidad.	Actividades de monitoreo y evaluación del cumplimiento de estándares de calidad y de líneas base de seguridad.
Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 11	Art. 37		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39		BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 23	Art. 6 Art. 8	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.	Art. 13	Art. 40 Art. 43 Art. 45 Art. 46	Art. 8	NO APLICA	NO APLICA
Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Art. 17	NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14		Art. 15	NO APLICA	NO APLICA
El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.	Art. 15	Art. 14	Art. 6 Art. 9 Art. 22 Art. 24 Art. 31 Art. 36 Art. 38	DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 17	Art. 25	Art. 11 Art. 18 Art. 19 Art. 34 Art. 37	NO APLICA	NO APLICA
Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 27 Art. 29	Art. 12	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.		Art. 24	Art. 10	NO APLICA	NO APLICA
Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener	Art. 19	Art. 47 Art. 57		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.					de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
				BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
				DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
				DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
				DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
				DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
				IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
				IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
				IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
				IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
				IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
				IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
				IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
				TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
				TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 9 Art. 48		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Organización.		Art. 48 - I		GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II		DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
				HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
				HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
				SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III		AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones
				GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información
Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV		NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V		AIS-01 Seguridad de la aplicación.	Consideraciones para el desarrollo seguro de aplicaciones.
				AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
				AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de información.
				CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
				CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI		AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
				GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
				TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
				TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII		SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
				SEF-02 Gestión de incidentes.	Políticas y procedimientos para la detección y manejo de incidentes de seguridad.
				SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII		DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
Establecer medidas para el aseguramiento de los		Art. 48 - IX		AIS-04 Seguridad de Datos /	Políticas y procedimientos para brindar

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.				Integridad.	confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
				BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
				DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
				DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
				DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
				EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
				IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
				IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
				IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
				IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
				IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
				IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
				IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
				TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
				TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
Establecer medidas para la trazabilidad de los datos		Art. 48 - X		AIS-04 Seguridad de Datos /	Políticas y procedimientos para brindar

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.				Integridad.	confidencialidad, integridad y disponibilidad de los datos.
				BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
				DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
				DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
				DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
				DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
				EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
				IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
				IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
				IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
				IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
				IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
				IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art 63 Art. 64		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
Los datos personales deben ser resguardados de tal manera que permitan el ejercicio de los derechos ARCO sin dilación de éstos.	Art. 22			BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Una vez cancelado el dato se dará aviso al su titular.	Art. 25			BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30			NO APLICA	NO APLICA
El responsable comunicará al titular, en un plazo máximo de 20 días, contados desde la fecha en que se recibió la solicitud ARCO, la determinación adoptada.	Art. 32			NO APLICA	NO APLICA

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Art. 15 Art. 26 Art. 27	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos, que complementen lo dispuesto por la Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia, consecuencias y medidas correctivas, en caso de incumplimiento.	Art. 44			Seguridad de la Aplicación y de Interfaz.	Conjunto de controles destinados a brindar seguridad a las aplicaciones y sus interfaces con otros sistemas.
				Aseguramiento de Auditoría y Cumplimiento.	Conjunto de controles para llevar a cabo la auditoría y revisión del cumplimiento de infraestructura de TI y de aplicaciones.
				Gestión de la Continuidad del Negocio y Capacidad de Recuperación Operacional.	Conjunto de controles para brindar continuidad del negocio y recuperación de los procesos que dependen de TI.
				Control de Cambios y Gestión de la Configuración.	Conjunto de controles para controlar cambios al ambiente operativo y gestionar la configuración de infraestructura de TI y aplicaciones.
				Seguridad de Datos y Gestión del Ciclo de Vida de la Información.	Conjunto de controles para brindar la seguridad de los datos y de la información durante su ciclo de vida.
				Seguridad del Centro de Datos.	Conjunto de controles físicos para la seguridad en los centros de datos.
				Gestión de Cifrado y Llaves.	Conjunto de controles para implementar cifrado de la información y gestión de las llaves de cifrado.
				Gobierno y Gestión de Riesgo.	Controles y actividades para gestión de riesgos de seguridad, y de cumplimiento regulatorio.
				Recursos Humanos.	Controles y prácticas para contar con seguridad en las relaciones con los empleados.
				Gestión de Identidades y Accesos.	Controles para la gestión de identidades de los usuarios y procesos, y el control de acceso a la infraestructura de TI y aplicaciones.
				Infraestructura y Seguridad en la Virtualización.	Controles para dar seguridad en ambientes virtualizados.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Interoperabilidad y Portabilidad.	Controles y prácticas para brindar interoperabilidad y portabilidad a las aplicaciones que funcionan en un esquema de cómputo en la nube.
				Seguridad Móvil.	Controles y prácticas para la seguridad por el uso de dispositivos móviles.
				Gestión de Incidentes de Seguridad, Forense en la Nube, y Descubrimiento Electrónico.	Controles y prácticas para la detección y atención de incidentes de seguridad.
				Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.	Gestión de terceros que participan como proveedores para brindar los servicios de cómputo en la nube a los clientes finales.
				Gestión de Amenazas y Vulnerabilidades.	Controles y prácticas para el manejo adecuado de amenazas y vulnerabilidades de seguridad informática.
La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				DSI-03 Transacciones de Comercio Electrónico	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.		Art. 52 - II		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo,		Art. 59		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
o bien, contratar a una persona física o moral para tal fin.				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: I. El riesgo inherente por tipo de dato personal; II. La sensibilidad de los datos personales tratados; III. El desarrollo tecnológico, y IV. Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.		Art. 60		AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I		DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II		HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
				HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
				HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
				SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
				TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
				TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del		Art. 61 - VI		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
análisis de brecha.					de los datos.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
Llevar a cabo revisiones o auditorías.		Art. 61 - VII		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
				GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
				SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
				SEF-02 Gestión de incidentes.	Políticas y procedimientos para la detección y manejo de incidentes de seguridad.
				SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
				TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
				TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII		HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
				HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
				HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
				SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX		BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Contar con una relación de las medidas de seguridad.		Art. 61		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
				BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
				BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
				CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
				DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
				DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
				DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
				EKM-03 Protección de datos sensibles.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
				IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
				IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
				IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
				IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
				IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
				IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
				IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62		AIS-01 Seguridad de la aplicación.	Consideraciones para el desarrollo seguro de aplicaciones.
				AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
				AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
				BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de información.
				CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
				CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
				DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
				DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
				GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
				GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66		AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el Reglamento y demás normativa aplicable.		Art. 70		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75		AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
				DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
				DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
				IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos.		Art. 80		Seguridad de la Aplicación y de Interfaz.	Conjunto de controles destinados a brindar seguridad a las aplicaciones y sus interfaces con otros sistemas.
				Aseguramiento de Auditoría y Cumplimiento.	Conjunto de controles para llevar a cabo la auditoría y revisión del cumplimiento de infraestructura de TI y de aplicaciones.
				Gestión de la Continuidad del Negocio y Capacidad de Recuperación Operacional.	Conjunto de controles para brindar continuidad del negocio y recuperación de los procesos que dependen de TI.
				Control de Cambios y Gestión de la Configuración.	Conjunto de controles para controlar cambios al ambiente operativo y gestionar la configuración de infraestructura de TI y aplicaciones.
				Seguridad de Datos y Gestión del Ciclo de Vida de la Información.	Conjunto de controles para brindar la seguridad de los datos y de la información durante su ciclo de vida.
				Seguridad del Centro de Datos.	Conjunto de controles físicos para la seguridad en los centros de datos.
				Gestión de Cifrado y Llaves.	Conjunto de controles para implementar cifrado de la información y gestión de las llaves de cifrado.
				Gobierno y Gestión de Riesgo.	Controles y actividades para gestión de riesgos de seguridad, y de cumplimiento regulatorio.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
				Recursos Humanos.	Controles y prácticas para contar con seguridad en las relaciones con los empleados.
				Gestión de Identidades y Accesos.	Controles para la gestión de identidades de los usuarios y procesos, y el control de acceso a la infraestructura de TI y aplicaciones.
				Infraestructura y Seguridad en la Virtualización.	Controles para dar seguridad en ambientes virtualizados.
				Interoperabilidad y Portabilidad.	Controles y prácticas para brindar interoperabilidad y portabilidad a las aplicaciones que funcionan en un esquema de cómputo en la nube.
				Seguridad Móvil.	Controles y prácticas para la seguridad por el uso de dispositivos móviles.
				Gestión de Incidentes de Seguridad, Forense en la Nube, y Descubrimiento Electrónico.	Controles y prácticas para la detección y atención de incidentes de seguridad.
				Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.	Gestión de terceros que participan como proveedores para brindar los servicios de cómputo en la nube a los clientes finales.
				Gestión de Amenazas y Vulnerabilidades.	Controles y prácticas para el manejo adecuado de amenazas y vulnerabilidades de seguridad informática.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable pondrá a disposición del titular para el ejercicio de sus derechos ARCO, medios remotos o locales de comunicación electrónica u otros que considere pertinentes. Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.		Art. 90	Art. 28	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				DSI-07 Propiedad / Custodia.	Definición y establecimiento de la propiedad y custodia de los datos e información.
Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley.		Art. 91		NO APLICA	NO APLICA
El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.		Art. 93		NO APLICA	NO APLICA
El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.		Art. 95		DSI-07 Propiedad / Custodia.	Definición y establecimiento de la propiedad y custodia de los datos e información.
En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.		Art. 98		AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				DSI-07 Propiedad / Custodia.	Definición y establecimiento de la propiedad y custodia de los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá: I. Atender las medidas de seguridad adecuadas para el bloqueo; II. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas.		Art. 107		BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.		Art. 110	Art. 25 Art. 30	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
				DSI-07 Propiedad / Custodia.	Definición y establecimiento de la propiedad y custodia de los datos e información.

Requerimiento LFPDPPP	Referencia LFPDPPP	Referencia Reglamento	Referencia Lineamientos	Identificador y Nombre Objetivo de Control	Descripción
El responsable estará obligado a poner a disposición de los titulares un nuevo aviso de privacidad, de conformidad con lo que establece la Ley, su Reglamento y los Lineamientos, cuando el responsable: I. Cambie su identidad; II. Requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento; III. Cambie las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular; o bien, se incorporen nuevas que requieran del consentimiento del titular, o IV. Modifique las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.			Art. 33	NO APLICA	NO APLICA

5. ANEXO

Las definiciones aquí enunciadas derivan de conceptos relevantes de conformidad con la Ley Federal de Protección de Datos en Posesión de los Particulares y su Reglamento, y las cuales a saber, son las siguientes:

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con la obligación establecida en la Ley.

Bases de Datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Confidencialidad: Proteger la información de su divulgación no autorizada. Esto significa que la información debe estar protegida de ser conocida por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos Personales Sensibles: Aquellos Datos Personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición que los titulares tienen respecto de sus Datos Personales que trata el Responsable.

Disponibilidad: Se refiere a que la información sea accesible cuando sea requerida.

Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Instituto: Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Integridad: Proteger la información de alteraciones no autorizadas.

Ley ó LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Protección de Datos Personales: La totalidad de medidas encaminadas a asegurar los derechos de los titulares en el tratamiento de sus datos personales.

Reglamento: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Titular: La persona física a quien corresponden los datos personales, sensibles y/o patrimoniales.

Transferencia: Toda comunicación de datos personales realizada a persona distinta del Responsable o Encargado del tratamiento.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. En el entendido que el uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de Datos Personales.