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

Introducción. COBIT 4.1 es un marco de referencia para la implementación del gobierno y gestión de los recursos de TI en las organizaciones. Su objetivo es proporcionar valor a la organización por medio de un coste óptimo de recursos, a la vez que los riesgos son controlados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	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.	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	Definición de políticas y procedimientos de gestión de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					servicio.	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.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	hacerse a través de medios engañosos o fraudulentos.					
CONSENTIMIENTO						
3	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 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	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. 56	Paso 2. Política de Gestión de Datos Personales.	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.
6	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	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	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	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	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.
					PO2.2 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.
					PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						y sensible es la información de la empresa.
					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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	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. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	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.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	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	Definir e implementar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Almacenamiento y Conservación.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de los datos.
14	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.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.				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.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	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.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos	PO4.14 Políticas y Procedimientos para	Asegurar que los consultores y el personal contratado que soporta

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.			Personales.	Personal Contratado.	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.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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.				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	Optimizar el uso de la información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					datos.	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.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	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	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de los sistemas.	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.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
21	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.	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.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías		Art. 48 - III	Paso 8. Revisiones y Auditoría.	PO8.6 Medición, Monitoreo y Revisión	Definir, planear e implementar mediciones para monitorear el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	externas para comprobar el cumplimiento de las políticas de privacidad.				de la Calidad.	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.
23	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.	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.
24	Instrumentar un procedimiento para que se		Art. 48 - V	Paso 5. Realizar el	PO9 Evaluar y	La elaboración de un marco de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.			Análisis de Riesgo de los Datos Personales.	Administrar los Riesgos de TI.	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.
					DS5.1 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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
26	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.	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.
					DS8.3 Escalamiento	Establecer procedimientos de mesa de servicios de manera que

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de Incidentes.	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.
27	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. Funciones y Obligaciones de Quienes Traten Datos Personales.	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	Definir claramente y comunicar las características de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Seguridad.	seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
28	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.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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
					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	Definir e implementar las políticas y procedimientos para identificar y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Seguridad para la Administración de Datos.	aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
29	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.	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.
					DS11.1 Requerimientos del Negocio para	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Administración de Datos.	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.
30	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.	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.
					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.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de	PO2.3 Esquema de Clasificación de	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.			seguridad y Análisis de Brecha.	Datos.	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.
					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	Proteger los activos de cómputo y la información del negocio

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					ambiente físico.	minimizando el riesgo de una interrupción del servicio.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. 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	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				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.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	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.
					DS11.3 Sistema de	Definir e implementar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Administración de Librerías de Medios.	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.
34	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.	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.
35	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.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						para el desarrollo de los requerimientos.
36	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.	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.
					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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
37	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	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.	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.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	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.
41	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
43	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. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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.
VULNERACIONES A LA SEGURIDAD						
44	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	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.	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.
46	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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.
ENCARGADO						
47	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		Art. 50	1. Recomendación General.	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.
					DS1 Definir y administrar los niveles	Identificación de requerimientos de servicio, el acuerdo de niveles

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				de servicio.	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.
SUBCONTRATACIONES						
48	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.	DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
49	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. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	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		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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.
					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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				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.
51	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	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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.					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.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	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	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas 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.
53	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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	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	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.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de	DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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.