4.2 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.

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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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	Actividades para la gestión de incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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.
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 hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	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 para prevenir brechas relacionadas a la seguridad de información personal
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	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
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.	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 para prevenir brechas relacionadas a la seguridad de información personal
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	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	que persigue el sujeto regulado.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
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 Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
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.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
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 Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
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	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

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.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
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.	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 para prevenir brechas relacionadas a la seguridad de información personal
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	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.					utilizados.
					11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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 para prevenir brechas relacionadas a la seguridad de información personal
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.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
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	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obtener nuevamente el consentimiento del titular. 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.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
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.	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 para prevenir brechas relacionadas a la seguridad de información personal.
CONFIDENCIALIDAD						
17	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. Política de Gestión de Datos Personales.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
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. 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. 47	Paso 2. Política de Gestión de Datos Personales.	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.

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
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.	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	Actividades para prevenir brechas relacionadas a la seguridad de información

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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 para prevenir brechas relacionadas a la seguridad de información personal
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.	7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Información.	seguridad de la información.
22	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.	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.
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.	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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
24	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.	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.
					18.2.1 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.

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	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.
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.	7.2.3 Proceso disciplinario.	Actividades para el establecimiento de un proceso disciplinario en caso de violaciones a la seguridad de la información.
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.	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.

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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.
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.	8.3.1 Gestión de medios removibles.	Lineamientos para la implementación de procedimientos para la gestión de medios removibles.
					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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					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.
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.	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.
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	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información

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.		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

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 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. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	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.
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.	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
					6.1.1 Roles y responsabilidades de	Todas los roles y responsabilidades deben ser

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal.
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.	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 para 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.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	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.
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.	12.6.1 Gestión de vulnerabilidades técnicas.	Actividades para identificar y prevenir que las vulnerabilidades técnicas en los activos de información sean explotadas.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	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	La organización debe someterse

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						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.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	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.
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		Art. 62	Paso 8. Revisiones y Auditoría.	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,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
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.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
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.	16.1.5 Respuesta a incidentes de Seguridad de la Información.	Procedimientos para la respuesta a incidentes de seguridad.
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.	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.
ENCARGADO						

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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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. Cumplimiento Cotidiano de Medidas de Seguridad.	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 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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
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.	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.
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 d) Guardar confidencialidad respecto de los		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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 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.
					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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales sobre los que se preste el servicio.				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 para prevenir brechas relacionadas a la seguridad de información personal.
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;		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	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.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	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.				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 para prevenir brechas relacionadas a la seguridad de información personal
TRANSFERENCIAS						
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	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 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 para prevenir brechas relacionadas a la seguridad de información personal
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.	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.

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	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.
55	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.	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.