

## 4.22 ITIL, Information Technology Infrastructure Library v3.

**Introducción.** Es un conjunto de conceptos y prácticas en la gestión de servicios de tecnologías de la información, para lograr calidad y eficiencia en las operaciones. Su propósito fundamental es servir como guía para toda infraestructura, desarrollo y operación de Tecnología de la Información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
<b>RESPONSABLE</b>						
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.	Estrategia del Servicio.  Diseño del Servicio.  Transición del Servicio.  Operación del Servicio.  Mejora continua del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.  Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.  Procesos requeridos para colocar un servicio de TI de manera operacional.  Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.  Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
<b>LICITUD Y LEALTAD</b>						
2	<p>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.</p> <p>La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.</p>	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
<b>CONSENTIMIENTO</b>						
3	<p>El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.</p> <p>Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular.</p> <p>Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.</p>	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	<p>Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.</p> <p>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.</p>	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
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.	NO APLICA	NO APLICA
<b>INFORMACIÓN</b>						
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.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>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.</p> <p>Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.</p>					
8	<p>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.</p>	<p>Art. 3, I Art. 17</p>	<p>Art. 27</p>	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	<p>NO APLICA</p>	<p>NO APLICA</p>
9	<p>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.</p>	<p>Art. 18</p>	<p>Art. 14 Art. 29 Art. 32</p>	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento</p>	<p>NO APLICA</p>	<p>NO APLICA</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad		
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
<b>CALIDAD</b>						
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.	SD3.6 Aspectos de diseño. SD3.6.3 Diseño de la arquitectura tecnológica. SD3.9 Arquitectura orientada al servicio.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida. Prácticas para el diseño de la arquitectura tecnológica que cubra las necesidades presentes y futuras del negocio. Prácticas para que los procesos y soluciones de negocio cuenten con un enfoque de arquitectura orientada al servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SD3.10 Gestión de servicio al negocio.	Prácticas para que los componentes de TI se encuentren ligados a los objetivos y metas del negocio.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					ST4.7 Gestión del conocimiento.	Prácticas recomendadas para la gestión del conocimiento necesario para la toma de decisiones.
					SD7 Consideraciones tecnológicas.	Recomendaciones para el uso de herramientas y técnicas en el diseño de servicios.
					SS6.5 Estrategia de sourcing.	Recomendaciones para definir la estrategia de outsourcing.
					SD3.5 Actividades de diseño.	Procesos principales para el diseño de servicios de TI.
					SD3.9 Arquitectura orientada al servicio.	
					SD3.11 Modelos para el diseño de los servicios.	Consideraciones para la adopción de un modelo para el diseño de los servicios.
					SD5.3 Gestión de aplicaciones.	Prácticas para la gestión efectiva de aplicaciones.
					ST3.2.3 Adopción de estándares y de un	Lineamientos para adoptar un estándar y un marco de trabajo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					marco de trabajo común.	común para la transición de servicios de TI.
					ST4.1.5.1 Estrategia de transición.	Recomendaciones para la adopción de una estrategia de transición de servicios de TI.
12	<p>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.</p> <p>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.</p>	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
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.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
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.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
					SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
<b>FINALIDAD</b>						
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.  El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica,	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	sin que ello tenga como consecuencia la conclusión del tratamiento.					
<b>PROPORCIONALIDAD</b>						
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.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
<b>CONFIDENCIALIDAD</b>						
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.	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
<b>RESPONSABILIDAD</b>						
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.	Estrategia del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.
	El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el				Diseño del Servicio.	Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				Transición del Servicio.	Procesos requeridos para colocar un servicio de TI de manera operacional.
					Operación del Servicio.	Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.
					Mejora continua del Servicio.	Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.
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.	SS7.5 Estrategia y mejora. SS9.5 Riesgos. SD2.4.2 Alcance. SD3.6 Aspectos de diseño. SD4.5.5.2 Etapa 2 – Requisitos y estrategia. SD4.6 Gestión de la	Aspectos de calidad al cliente a considerar en la definición de la estrategia del servicio de TI. Identificación de tipos de riesgos a ser identificados y controlados. Aspectos para la definición del alcance del diseño del servicio. Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida. Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio. Prácticas recomendadas para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información.	gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					Apéndice E Detalles de la gestión de las instalaciones.	Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.
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.	SS6.4 Cultura organizacional.	Aspectos para incrementar la efectividad organizacional.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
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.	SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						implementación.
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.	CSI5.2 Evaluaciones. CSI5.3 Benchmarking. CSI5.4 Marcos de medición y reporte. SO4.5.5.6 Eliminar o restringir privilegios. SO5.13 Gestión de seguridad de la información y la operación del servicio.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización. Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado. Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales. Aspectos a considerar en la eliminación o restricción de los privilegios de acceso. Aspectos fundamentales de la seguridad de la información en la operación del servicio.
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.	SD4.6 Gestión de seguridad de la información. SO5.13 Gestión de seguridad de la información y la operación del servicio.	Prácticas recomendadas para la gestión de la seguridad de la información. Aspectos fundamentales de la seguridad de la información en la operación del servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
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.	SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD4.6.4 Políticas,	Conceptos básicos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					principios y conceptos básicos.	seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	CSIS.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSIS.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSIS.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.

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.	SO4.1 Gestión de eventos. SO4.2 Gestión de incidentes. SO6.2 Mesa de servicios.	Prácticas para la gestión de eventos en los servicios de TI. Prácticas para la gestión de incidentes en los servicios de TI. Prácticas para la atención de eventos y solicitudes en los servicios de TI.
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.	SD4.6.4 Políticas, principios y conceptos básicos. SD4.6.5.1 Controles de seguridad. SO4.5.5.6 Eliminar o restringir privilegios. SO5.13 Gestión de seguridad de la información y la operación del servicio. SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Conceptos básicos de seguridad de la información para ser implementados. Tipos de controles de seguridad recomendados para su implementación. Aspectos a considerar en la eliminación o restricción de los privilegios de acceso. Aspectos fundamentales de la seguridad de la información en la operación del servicio. Consideraciones para la gestión de brechas e incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					ST3.2.13 Asegurar la calidad de un servicio nuevo o modificado.	Principios y mejores prácticas para lograr la calidad de un servicio nuevo o modificado.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.12 Gestión del	Aspectos a considerar para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					centro de datos e instalaciones.	gestión eficiente del centro de datos y las instalaciones.
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.	SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
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.	SD6.4 Roles y responsabilidades.	Roles y responsabilidades para el diseño de servicios de TI.
					SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
<b>SEGURIDAD</b>						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>o el uso, acceso o tratamiento no autorizado.</p> <p>No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información.</p> <p>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.</p>				<p>SD4.6 Gestión de la seguridad de la información.</p> <p>SD5.2 Gestión de los datos y la información.</p> <p>Apéndice E Detalles de la gestión de las instalaciones.</p>	<p>Prácticas recomendadas para la gestión de la seguridad de la información.</p> <p>Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.</p> <p>Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.</p>
32	<p>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.</p> <p>De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:</p> <p>I. El número de titulares;</p> <p>II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;</p> <p>III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una</p>	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	<p>SS9.5 Riesgos.</p> <p>SD4.5.5.1 Etapa 1 – Inicio.</p> <p>SD2.4.2 Alcance.</p> <p>SD3.6 Aspectos de diseño.</p> <p>SD4.5.5.2 Etapa 2 – Requisitos y</p>	<p>Identificación de tipos de riesgos a ser identificados y controlados.</p> <p>Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.</p> <p>Aspectos para la definición del alcance del diseño del servicio.</p> <p>Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.</p> <p>Prácticas para el desarrollo de un Análisis de Impacto al</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>tercera persona no autorizada para su posesión, y</p> <p>IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.</p>				<p>estrategia.</p> <p>SD3.6.1 Diseño de soluciones de servicios.</p> <p>SO4.4.5.11 Errores detectados en el entorno de desarrollo.</p> <p>SD4.6.4 Políticas, principios y conceptos básicos.</p> <p>SD4.6.5.1 Controles de seguridad.</p> <p>SD5.2 Gestión de los datos y la información.</p>	<p>Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.</p> <p>Actividades de diseño para un servicio nuevo o modificado.</p> <p>Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.</p> <p>Conceptos básicos de seguridad de la información para ser implementados.</p> <p>Tipos de controles de seguridad recomendados para su implementación.</p> <p>Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.</p>
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	<p>SD5.2 Gestión de los datos y la información.</p> <p>ST4.3.5.3 Identificación de la configuración.</p>	<p>Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.</p> <p>Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SO5.2.4 Datos electrónicos e impresos.	Prácticas para el manejo de datos en formato electrónico e impreso.
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.	SO6.3 Gestión técnica.	Roles y responsabilidades para la gestión de la infraestructura de TI.
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.	SS9.5 Riesgos. SD4.5.5.1 Etapa 1 – Inicio. SD2.4.2 Alcance. SD3.6 Aspectos de diseño. SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Identificación de tipos de riesgos a ser identificados y controlados. Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI. Aspectos para la definición del alcance del diseño del servicio. Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida. Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar		Art. 61 - IV	Paso 6. Identificación de las	SD3.6.1 Diseño de soluciones de	Actividades de diseño para un servicio nuevo o modificado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	aquéllas implementadas de manera efectiva.			medidas de seguridad y Análisis de Brecha.	servicios.	
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.
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.	NO APLICA	NO APLICA

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.	NO APLICA	NO APLICA
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	CSIS.2 Evaluaciones. CSIS.3 Benchmarking. CSIS.4 Marcos de medición y reporte. SO4.5.5.6 Eliminar o restringir privilegios. SO5.13 Gestión de seguridad de la	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización. Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado. Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales. Aspectos a considerar en la eliminación o restricción de los privilegios de acceso. Aspectos fundamentales de la seguridad de la información en

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información y la operación del servicio.	la operación del servicio.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
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.	ST4.3.5.3 Identificación de la configuración.	Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SD5.2 Gestión de los datos y la	Prácticas recomendadas para la gestión de la seguridad de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información.	información.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
43	<p>Actualizar las medidas de seguridad cuando:</p> <p>I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.</p> <p>II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.</p> <p>III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.</p> <p>IV. Exista una afectación a los datos personales distinta a las anteriores.</p> <p>En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.</p>		Art. 62	Paso 8. Revisiones y Auditoría.	CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.
					SO5.7 Administración de bases de datos.	Prácticas recomendadas para la gestión de bases de datos.
					SO5.8 Gestión de servicios de directorio.	Prácticas recomendadas para la gestión de servicios de directorio.
					SO5.9 Soporte de estaciones de trabajo.	Actividades a considerar para el soporte de la operación de estaciones de trabajo.
					SO5.10 Gestión de middleware.	Prácticas recomendadas para la gestión de los componentes middleware de los servicios de TI.
					SO5.11 Gestión Internet/web.	Prácticas recomendadas para la gestión de servicios basados en web.
					SD4.6 Gestión de la	Prácticas recomendadas para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información	gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
<b>VULNERACIONES A LA SEGURIDAD</b>						
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.	SO4.5.5.6 Eliminar o restringir privilegios. SO5.13 Gestión de seguridad de la información y la operación del servicio. SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso. Aspectos fundamentales de la seguridad de la información en la operación del servicio. Consideraciones para la gestión de brechas e incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	<p>En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente:</p> <p>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.</p>		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
46	<p>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.</p>		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	SO4.5.5.6 Eliminar o restringir privilegios. SO5.13 Gestión de seguridad de la información y la operación del servicio. SD4.6.5.2 Gestión de brechas de seguridad e incidentes. SO4.4 Gestión de problemas.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso. Aspectos fundamentales de la seguridad de la información en la operación del servicio. Consideraciones para la gestión de brechas e incidentes de seguridad de la información. Prácticas para la gestión de problemas presentados en la operación de los servicios de TI.

ENCARGADO

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	<p>El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:</p> <p>I. Tratar únicamente los datos personales conforme a las instrucciones del responsable.</p> <p>II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.</p> <p>III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables.</p> <p>IV. Guardar confidencialidad respecto de los datos personales tratados.</p> <p>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.</p> <p>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.</p>		Art. 50	1. Recomendación General.	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
					SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
<b>SUBCONTRATACIONES</b>						

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.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
49	<p>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.</p> <p>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.</p> <p>En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente.</p> <p>La obligación de acreditar que la subcontratación se realizó con autorización</p>		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.					
<b>CÓMPUTO EN LA NUBE</b>						
50	<p>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:</p> <p>a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento;</p>		Art. 52 - I	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;</p> <p>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</p> <p>d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.</p>				<p>SD4.2 Gestión de niveles de servicios.</p> <p>SD4.7 Gestión de proveedores.</p> <p>SD4.6 Gestión de la seguridad de la información.</p> <p>SD5.2 Gestión de los datos y la información.</p> <p>SO5.12 Gestión del centro de datos e instalaciones.</p>	<p>Prácticas para la gestión de niveles de servicios.</p> <p>Prácticas para la gestión de proveedores.</p> <p>Prácticas recomendadas para la gestión de la seguridad de la información.</p> <p>Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.</p> <p>Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.</p>
51	<p>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:</p>		Art. 52 - II	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de</p>	<p>SD4.2.5.9 Desarrollar contratos y relaciones.</p> <p>SD4.7.5.3 Nuevos proveedores y contratos.</p>	<p>Consideraciones para establecer contratos y desarrollar relaciones con terceros.</p> <p>Aspectos para el manejo de nuevos proveedores y la formalización de contratos.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;</p> <p>b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;</p> <p>c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;</p> <p>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</p> <p>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.</p>			Medidas de Seguridad.	<p>SD4.2 Gestión de niveles de servicios.</p> <p>SD4.7 Gestión de proveedores.</p> <p>SD4.6 Gestión de la seguridad de la información.</p> <p>SD5.2 Gestión de los datos y la información.</p> <p>SO5.12 Gestión del centro de datos e instalaciones.</p>	<p>Prácticas para la gestión de niveles de servicios.</p> <p>Prácticas para la gestión de proveedores.</p> <p>Prácticas para la gestión de proveedores.</p> <p>Prácticas recomendadas para la gestión de la seguridad de la información.</p> <p>Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.</p>
<b>TRANSFERENCIAS</b>						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	<p>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.</p> <p>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.</p>	Art. 36	<p>Art. 68</p> <p>Art. 71</p> <p>Art. 72</p> <p>Art. 74</p>	<p>Paso 7.</p> <p>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.</p> <p>Cumplimiento Cotidiano de Medidas de Seguridad.</p>	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
53	<p>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.</p>		Art. 69	<p>Paso 7.</p> <p>Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.</p> <p>Cumplimiento Cotidiano de Medidas de Seguridad.</p>	SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.

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	SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
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.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.