

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

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

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.	<p>9.2.3.3.1 Cumplimiento legal y regulatorio.</p> <p>9.1.6 Reporte de auditoría de certificación.</p> <p>9.3 Actividades de supervisión.</p> <p>9.4 Recertificación.</p> <p>10.3.1 Implementación de un Sistema de Gestión de Seguridad</p>	<p>Establece la responsabilidad del cumplimiento legal y regulatorio.</p> <p>Describe los elementos que componen un reporte de auditoría de certificación.</p> <p>Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.</p> <p>Describe las circunstancias y condiciones para mantener la certificación.</p> <p>Recomienda la implementación del sistema de gestión con base en ISO 27001.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de la Información.	
<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.	NO APLICA	NO APLICA
<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.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.  No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
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	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>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.</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>			Personales.		
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>	Art. 3, I Art. 17	Art. 27	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	NO APLICA	NO APLICA
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</p>	Art. 18	Art. 14 Art. 29 Art. 32	<p>Paso 7. Implementación de las Medidas de Seguridad</p>	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.			Aplicables a los Datos Personales. Cumplimiento 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.	NO APLICA	NO APLICA
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,	Art. 3 III Art. 11	Art. 37	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>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>					
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.	NO APLICA	NO APLICA
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
<b>FINALIDAD</b>						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
15	<p>El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.</p> <p>Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.</p> <p>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.</p>	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
<b>PROPORCIONALIDAD</b>						
16	<p>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.</p>	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
<b>CONFIDENCIALIDAD</b>						
17	<p>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.</p>	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
<b>RESPONSABILIDAD</b>						
<b>18</b>	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.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
<b>19</b>	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.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de		Art. 48 - III	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	las políticas de privacidad.				9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	7.1.1.1 Análisis de competencias y revisión contractual.	Establece el proceso de revisión de la organización cliente en cuanto a sus riesgos y su competencia en seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.
					9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
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.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
<b>SEGURIDAD</b>						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	<p>Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.</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>	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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>	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.					
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación. 9.1.2 Alcance de la certificación.	Establece como criterio de auditoría al utilizado en ISO 27001. Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						especial.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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>		Art. 62	Paso 8. Revisiones y Auditoría.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<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>					
<b>VULNERACIONES A LA SEGURIDAD</b>						
44	<p>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.</p>	Art. 20	Art. 63 Art. 64	<p>Paso 8. Revisiones y Auditoría.</p> <p>Vulneraciones a la Seguridad de la Información.</p>	NO APLICA	NO APLICA
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.</p> <p>II. Los datos personales comprometidos.</p> <p>III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.</p> <p>IV. Las acciones correctivas realizadas de forma inmediata.</p> <p>V. Los medios donde puede obtener más</p>		Art. 65	<p>Paso 8. Revisiones y Auditoría.</p> <p>Vulneraciones a la Seguridad de la Información.</p>	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	información al respecto.					
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. Revisión y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
<b>ENCARGADO</b>						
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		Art. 50	1. Recomendación General.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>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>					
<b>SUBCONTRATACIONES</b>						
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	<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>	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 del responsable corresponderá al encargado.</p>		Art. 54 Art. 55	<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>	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
<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</p>		Art. 52 - I	<p>Paso 7.</p> <p>Implementación de las Medidas de Seguridad Aplicables a los</p>	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>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> <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>Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	<p>8.5 Confidencialidad.</p>	<p>Establece la protección de registros confidenciales del sistema de gestión.</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</p>		<p>Art. 52 - II</p>	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.</p>	<p>10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.</p>	<p>Recomienda la implementación del sistema de gestión con base en ISO 27001.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>servicios en los que el proveedor cuente con mecanismos, al menos, para:</p> <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>			<p>Cumplimiento Cotidiano de Medidas de Seguridad.</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 Art. 71 Art. 72 Art. 74</p>	<p>Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
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. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.</p>	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.

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	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
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.	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.