

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

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

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.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
					6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado al cumplimiento de los objetivos de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
					8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
<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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
<b>CONSENTIMIENTO</b>						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.				Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.	
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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.				Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
<b>INFORMACIÓN</b>						
7	<p>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.</p> <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>	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
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	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
<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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
<b>FINALIDAD</b>						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<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>				planeación para alcanzarlos.	objetivos.
<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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
<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.	5.2 Política.  6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	<p>La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.</p> <p>Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					6.1.3 Tratamiento de riesgos de Seguridad de la Información. / 8.3	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
<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.  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.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
					6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						al cumplimiento de los objetivos de la organización.
					7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
					8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2 Competencia.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad.
					7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
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.	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
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.	7.1 Recursos.	Asignación de los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora del ISMS.
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.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
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. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.

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.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
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.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.

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.	<p>5.2 Política.</p> <p>6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.</p> <p>6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.</p> <p>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p> <p>8.1 Planeación y Control Operacional.</p>	<p>La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.</p> <p>Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.</p> <p>Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.</p> <p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p> <p>Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.</p>
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		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento.			de Brecha.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
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.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.3 Roles, responsabilidades, y autoridades organizacionales.	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a seguridad de la información sean correctamente asignados y comunicados.
<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 o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<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>Información.</p> <p>6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.</p> <p>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p> <p>8.1 Planeación y Control Operacional.</p>	<p>aceptada por la dirección.</p> <p>Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.</p> <p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p> <p>Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.</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</p>	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	<p>4. Contexto de la Organización.</p> <p>6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.</p>	<p>Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.</p> <p>Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					5.3 Roles, responsabilidades, y autoridades	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					organizacionales.	seguridad de la información sean correctamente asignados y comunicados.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
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.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
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.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
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	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				para la Implementación de las Medidas de Seguridad Faltantes.		alinear los planes al logro de los objetivos del ISMS.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9. Evaluación del desempeño. 10. Mejora.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos. Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2 Competencia. 7.3 Concientización.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad. Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
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.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.
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.	8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
<b>VULNERACIONES A LA SEGURIDAD</b>						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente:  I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
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,		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.			Información.	10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
<b>ENCARGADO</b>						
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,</p>		Art. 50	1. Recomendación General.	<p>5.2 Política.</p> <p>6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.</p> <p>6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.</p> <p>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p> <p>8.1 Planeación y Control Operacional.</p>	<p>La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.</p> <p>Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.</p> <p>Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.</p> <p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p> <p>Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	o cuando así lo requiera la autoridad competente.					
<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	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
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</p>		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>correspondiente del responsable previamente.</p> <p>La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.</p>					
<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> <p>b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;</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>	<p>5.2 Política.</p> <p>6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.</p> <p>6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.</p>	<p>La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.</p> <p>Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.</p> <p>Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.</p>

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<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>				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
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> <p>a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;</p>		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<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>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p> <p>8.1 Planeación y Control Operacional.</p>	<p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p> <p>Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.</p>
<b>TRANSFERENCIAS</b>						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	<p>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>			<p>Datos Personales.</p> <p>Cumplimiento Cotidiano de Medidas de Seguridad.</p>	<p>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p>	<p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p>
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>	<p>6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.</p>	<p>Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.</p>

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	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
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.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.