4.13 BS 10012:2009 Data Protection – Specification for a Personal Information Management System (PIMS).

Introducción. Introducción. Este estándar británico ha sido producido para formar las bases para las políticas internas sobre la legislación de protección de datos y el cumplimiento con las buenas prácticas. Asimismo, es un marco de referencia estándar para auditorías y procesos de revisión respecto a protección de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
					4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
					5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
					6 Mejora de un Sistema de Gestión de Información	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Personal.	relevantes.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	4.7 Procesamiento justo y lícito.	Actividades para que el procesamiento de información recopilada sea de forma licita y justa.
					4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionados.
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.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
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	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
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.	4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
					4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.
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.	4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
CALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
					4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
					4.10 Precisión.	Actividades para el mantenimiento íntegro y actualizado de los datos recopilados.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.

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.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
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.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. 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	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	4.8 Procesamiento de información personal para propósitos especificados.	Actividades para asegurar que la información obtenida es utilizada solo para los propósitos especificados.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	4.9 Idoneidad, relevante y no excesivo.	Actividades para asegurar que la información personal es adecuada, relevante y no excesiva.
					4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
					4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						vigentes.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
					4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
					5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
					6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.
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.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionados a la información personal.
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
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.	3.3 Política de gestión de información personal.	La dirección de la organización debe mantener y demostrar compromiso con una política de gestión de información personal.
					3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
					3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
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.	3.6 Provisión de recursos.	La organización determina y provee los recursos necesarios para el mantenimiento del PIMS.
					3.7 Incrustación del Sistema de Gestión de Información Personal en la cultura de la organización.	Actividades para incluir el PIMS como un valor relevante dentro de la organización

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
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.	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
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.	4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
					4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
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	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.	4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
SEGURIDAD						
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. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
					4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
					4.2.1 General.	Debe ser mantenido un inventario de las categorías de información personal

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
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.	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
					4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
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.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
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.	4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
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.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
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.	5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.
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.	4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el		Art. 62	Paso 8. Revisiones y Auditoría.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que		Art. 51	Paso 7. Implementación de las Medidas de Seguridad	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permita acreditar su existencia, alcance y contenido.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
51	Para el tratamiento de datos personales en		Art. 52 - II	Paso 7.	4.7.1 Recolección y	Procedimientos para asegurar el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de			Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	procesamiento de información personal.	cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
			TRANSFERENCIAS			
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.
					4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obligaciones que correspondan al responsable que transfirió los datos.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
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		Art. 70	1. Recomendación General	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
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.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.