4.23 The Open Web Application Security Project (OWASP), Guía de Documentación v2.0.

Introducción. OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen al software inseguro. La Guía de Documentación provee lineamientos detallados sobre la seguridad de las aplicaciones web.

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.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
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.	NO APLICA	NO APLICA
CONSENTIMIENTO						

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. 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.	NO APLICA	NO APLICA
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		Art. 20	Paso 7. Implementación de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	recaerá, en todos los casos, en el responsable.			las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
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.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.			Seguridad Aplicables a los Datos Personales. 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	NO APLICA	NO APLICA
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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
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.	NO APLICA	NO APLICA
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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	NO APLICA	NO APLICA
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 conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	NO APLICA	NO APLICA
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.	NO APLICA	NO APLICA
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	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
					Pilares esenciales de la seguridad de la información.	Consideraciones de la integridad, disponibilidad, y confidencialidad de la información para la producción de un control robusto de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	relación jurídica.				Arquitectura de seguridad.	Integración de los pilares de integridad, disponibilidad, y confidencialidad de la información en el desarrollo de aplicaciones.
					Principios de seguridad.	Lineamientos fundamentales para el desarrollo seguro de aplicaciones.
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.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
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.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
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.	Educación del usuario.	Consideraciones para entrenar a los usuarios con respecto a la seguridad de la información.

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.	NO APLICA	NO APLICA
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.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
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.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	NO APLICA	NO APLICA

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.	NO APLICA	NO APLICA
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.	NO APLICA	NO APLICA
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.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio	Manejo de los pagos de una manera segura en sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					electrónico.	comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
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.	Manejo de errores, auditoría, y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
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.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de	Guías para que la aplicación sea robusta frente a ataques de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					servicio.	negación de servicio.
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.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
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.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
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.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	NO APLICA	NO APLICA
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
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.	Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	NO APLICA	NO APLICA
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 artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62	Paso 8. Revisiones y Auditoría.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					
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.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
					Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
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.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades 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.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
					Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las		Art. 50	1. Recomendación General.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.					amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
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 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.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	NO APLICA	NO APLICA
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.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
51	Para el tratamiento de datos personales en		Art. 52 - II	Paso 7.	Arquitectura y diseño	Consideraciones para 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.	de seguridad.	establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones

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.					previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 obligaciones que correspondan al responsable que transfirió los datos.	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.	NO APLICA	NO APLICA
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.	NO APLICA	NO APLICA

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	NO APLICA	NO APLICA
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.	NO APLICA	NO APLICA