4.19 PCI DSS, Payment Card Industry Data Security Standard v2.0.

Introducción. Este estándar fue desarrollado por un comité conformado por las compañías de tarjetas bancarias más importantes, como una guía para las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, con el fin de asegurar dichos datos y prevenir fraudes.

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.	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
					Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
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	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	3.2 No almacene datos confidenciales de autenticación después de recibir la autorización.	Guías para el borrado seguro de datos confidenciales del tarjetahabiente cuando ya no son necesarios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.					
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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
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.	NO APLICA	NO APLICA
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, 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.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.

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.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
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.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
FINALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
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.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
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.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del	Guías para protección de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					titular de la tarjeta.	del tarjetahabiente.
	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.				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					riesgos para vulnerabilidades de seguridad descubiertas recientemente.	
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.	12.1 Establezca, publique, mantenga y distribuya una política de seguridad.	Guías para la definición y comunicación de la política de seguridad.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
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.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una	Guías para la revisión de seguridad ante modificaciones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					vez al año y actualizaciones al modificarse el entorno.	importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
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.	12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.
					12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los	Implementación del programa de concienciación de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					datos de titulares de tarjetas.	
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.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una	Guías para la revisión de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					revisión al menos una vez al año y actualizaciones al modificarse el entorno.	seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
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.	12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información de todo el 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.	Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas	Guías para el cifrado de datos durante su transmisión por redes abiertas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					abiertas.	
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten		Art. 48 - X	Paso 6. Identificación de las medidas de	10.2 Implemente pistas de auditoría automatizadas para	Guías para la verificación de pistas de auditoría en los sistemas y aplicaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	rastrear a los datos personales durante su tratamiento.			seguridad y Análisis de Brecha.	todos los componentes del sistema.	
					10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.	Guías para el resguardo de las pistas de auditoría.
					10.6 Revise los registros de todos los componentes del sistema al menos una vez al día.	Guías para el monitoreo de los componentes de los sistemas.
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.	12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo.	Guías para la asignación de un responsable de la seguridad de la información en la organización.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá	Art. 19	Art. 4 Art. 9	Paso 6. Identificación de las	Requisito 1: Instale y mantenga una	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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. 57	medidas de seguridad y Análisis de Brecha.	configuración de firewalls para proteger los datos de los titulares de las tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los	Guías para la operación y mantenimiento de los esquemas de antivirus.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					programas antivirus.	
					Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					tarjetas.	
					Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.

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.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	9.7.1 Clasifique los medios de manera que se pueda determinar la	Guías para la clasificación de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					confidencialidad de los datos.	
					9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
					9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.

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.	12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
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	Requisito 1: Instale y mantenga una configuración de firewalls para	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				de Brecha.	proteger los datos de los titulares de las tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6:	Guías para el desarrollo de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Desarrolle y mantenga sistemas y aplicaciones seguras.	aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe	Guías para revisar periódicamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					con regularidad los sistemas y procesos de seguridad.	la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
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.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una	Guías para llevar a cabo una evaluación formal de riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					evaluación formal de riesgos.	
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
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.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					modificarse el entorno.	del tarjetahabiente.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
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	9.7.1 Clasifique los medios de manera que se pueda	Guías para la clasificación de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Personales.	determinar la confidencialidad de los datos.	
					9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
					9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6: Desarrolle y mantenga sistemas y	Guías para el desarrollo de aplicaciones seguras.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					aplicaciones seguras.	
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe con regularidad los sistemas y procesos	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de seguridad.	de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
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.		Art. 62	Paso 8. Revisiones y Auditoría.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
					Requisito 11: Pruebe con regularidad los sistemas y procesos	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				de seguridad.	de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
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.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a 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.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a 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.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 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		Art. 50	1. Recomendación General.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	competente.					
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.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	
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		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.				Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.
CÓMPUTO EN LA NUBE						
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		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				tarjetas que ellos tienen en su poder.	
					12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.
					Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: 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		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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 acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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 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.	12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
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	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
					Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.