4.24 Cloud Security Alliance Cloud Controls Matrix (CCM) v3.0.

Introducción. Esta matriz proporciona principios de seguridad para evaluar el riesgo de seguridad en un proveedor de cómputo en la nube. El marco de trabajo del documento ofrece controles divididos en 13 dominios.

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.	Seguridad de la Aplicación y de Interfaz.	Conjunto de controles destinados a brindar seguridad a las aplicaciones y sus interfaces con otros sistemas.
					Aseguramiento de Auditoría y Cumplimiento.	Conjunto de controles para llevar a cabo la auditoría y revisión del cumplimiento de infraestructura de TI y de aplicaciones.
					Gestión de la Continuidad del Negocio y Capacidad de Recuperación Operacional.	Conjunto de controles para brindar continuidad del negocio y recuperación de los procesos que dependen de TI.
					Control de Cambios y Gestión de la Configuración.	Conjunto de controles para controlar cambios al ambiente operativo y gestionar la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						configuración de infraestructura de TI y aplicaciones.
					Seguridad de Datos y Gestión del Ciclo de Vida de la Información.	Conjunto de controles para brindar la seguridad de los datos y de la información durante su ciclo de vida.
					Seguridad del Centro de Datos.	Conjunto de controles físicos para la seguridad en los centros de datos.
					Gestión de Cifrado y Llaves.	Conjunto de controles para implementar cifrado de la información y gestión de las llaves de cifrado.
					Gobierno y Gestión de Riesgo.	Controles y actividades para gestión de riesgos de seguridad, y de cumplimiento regulatorio.
					Recursos Humanos.	Controles y prácticas para contar con seguridad en las relaciones con los empleados.
					Gestión de Identidades y Accesos.	Controles para la gestión de identidades de los usuarios y procesos, y el control de acceso a la infraestructura de TI y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						aplicaciones.
					Infraestructura y Seguridad en la Virtualización.	Controles para dar seguridad en ambientes virtualizados.
					Interoperabilidad y Portabilidad.	Controles y prácticas para brindar interoperabilidad y portabilidad a las aplicaciones que funcionan en un esquema de cómputo en la nube.
					Seguridad Móvil.	Controles y prácticas para la seguridad por el uso de dispositivos móviles.
					Gestión de Incidentes de Seguridad, Forense en la Nube, y Descubrimiento Electrónico.	Controles y prácticas para la detección y atención de incidentes de seguridad.
					Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.	Gestión de terceros que participan como proveedores para brindar los servicios de cómputo en la nube a los clientes finales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Gestión de Amenazas y Vulnerabilidades.	Controles y prácticas para el manejo adecuado de amenazas y vulnerabilidades de seguridad informática.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	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.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
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						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.					
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
9	El aviso de privacidad debe contener un	Art. 18	Art. 14	Paso 7.	AIS-04 Seguridad de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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. 29 Art. 32	Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	Datos / Integridad.	brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					CCC-03 Prueba de Calidad.	Actividades de monitoreo y evaluación del cumplimiento de estándares de calidad y de líneas base de seguridad.
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	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	presente el mencionado incumplimiento.				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
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	BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
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.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
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.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
RESPONSABILIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
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.	GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
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.	DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
					HRS-10	Definición de un programa

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Entrenamiento / Concientización.	formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
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.	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	NO APLICA	NO APLICA
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.	AIS-01 Seguridad de la aplicación.	Consideraciones para el desarrollo seguro de aplicaciones.
					AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
					CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
					CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-04 Seguridad de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Datos / Integridad.	brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
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.	SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
					SEF-02 Gestión de incidentes.	Políticas y procedimientos para la detección y manejo de incidentes de seguridad.
					SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
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.	DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto		Art. 48 - IX	Paso 6. Identificación de las	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.			medidas de seguridad y Análisis de Brecha.		integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de	Procedimientos para evitar el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					personal no autorizado.	ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-07 Mantenimiento de	Políticas y procedimientos para el mantenimiento adecuado de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					equipo.	equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
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	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
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	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	seguridad contenidas en el Capítulo III de Reglamento.					del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.

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;	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y	HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Obligaciones de Quienes Traten Datos Personales.		empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
					HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes 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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones	Protección de los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de Comercio Electrónico.	utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
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	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad Faltantes.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
					SEF-02 Gestión de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					incidentes.	la detección y manejo de incidentes de seguridad.
					SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de la información en contratos laborales.
					HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
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.	BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de	Políticas y procedimientos para el mantenimiento adecuado de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					equipo.	equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
43	Actualizar las medidas de seguridad cuando:		Art. 62	Paso 8. Revisiones y	AIS-01 Seguridad de	Consideraciones para el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.			Auditoría.	la aplicación.	desarrollo seguro de aplicaciones.
					AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
					CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
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.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	V. Los medios donde puede obtener más información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						e información.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
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.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
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		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.			Seguridad.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					DSI-03 Transacciones de Comercio Electrónico	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política	Políticas y procedimientos para el etiquetado y manejo de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				de Seguridad.	datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						confidencialidad los datos e información.
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		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política	Políticas y procedimientos para el etiquetado y manejo de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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 acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				de Seguridad.	datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
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		Art. 70	1. Recomendación General	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	condiciones en las que el titular consintió el tratamiento de sus datos personales.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.