4.18 Control Objectives for Information and Related Technology (COBIT 5).

Introducción. COBIT 5 es un marco de referencia para la implementación del gobierno y gestión de los recursos de Tecnología de la Información en las organizaciones. Su objetivo es proporcionar valor a la organización por medio de un coste óptimo de recursos, a la vez que los riesgos son controlados. COBIT 5 toma en cuenta las versiones anteriores, y añade mejoras en procesos, prácticas, actividades, métricas, y modelos de madurez principalmente.

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.	APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
					APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
					BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
					DSS01 Gestionar las	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Operaciones.	procedimientos para la entrega de servicios de TI.
					DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
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.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los	Asegurar que los puestos de usuario final se encuentren

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					puestos de usuario final.	asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.					información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes,	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.					dominios negocio, información, datos, aplicaciones y tecnología.
					APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
					APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC
					APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	Criterios para incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollo de soluciones y los servicios ofrecidos.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.					dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
13	El responsable establecerá y documentará		Art. 38	Paso 2. Política de	APO03.02 Definir la	La arquitectura de referencia

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.			Gestión de Datos Personales.	arquitectura de referencia.	describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de	Asegurar el acceso a los activos de información por métodos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información.	apropiados.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					autorización.	
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.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los	Actividades para asegurar que la información de negocio puede ser

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					eventos y responsabilidades de información.	rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
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.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					activos de TI.	de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la	Criterios para que los usuarios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					identidad del usuario y el acceso lógico.	tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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.	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
					APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
					BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los	Criterios para la administración de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Proveedores.	proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
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.	APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
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.	EDM03.02 Orientar la gestión de riesgos.	Orientar el establecimiento de prácticas de gestión de riesgos a asegurar que no se exceda el apetito del riesgo.
					APO01.03 Mantener los elementos catalizadores del sistema de gestión.	Actividades para el mantenimiento de elementos catalizadores dentro de los objetivos de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades dentro de la organización.
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.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
					DSS05.07 Supervisar la infraestructura para detectar eventos	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					relacionados con la seguridad.	accesos no autorizados y asegurar que cualquier evento esté contemplado.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
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.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
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.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los	Identificar, documentar, priorizar y mitigar los riesgos funcionales y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					requerimientos.	técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					final.	la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
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.	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
					DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	Procedimientos para el registro y gestión de incidentes.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS02.04 Investigar, diagnosticar y localizar incidentes.	Procedimientos para el diagnóstico, investigación y localización de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						seguridad.
					DSS02.05 Resolver y recuperarse de incidentes.	Procedimientos para la resolución y recuperación de servicios afectados por incidentes de seguridad.
					DSS02.06 Cerrar peticiones de servicio e incidentes.	Criterios para el cierre de incidentes y solicitudes de servicio.
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.	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					APO03.05 Proveer los servicios de arquitectura empresarial.	Guías de los proyectos, formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura.
					APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
					BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis	BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento.			de Brecha.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar	Criterios para el establecimiento

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					roles, responsabilidades, privilegios de acceso y niveles de autorización.	de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
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	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS06 Gestionar los Controles de los	Criterios para la definición y mantenimiento de controles a lo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Procesos de la Empresa.	largo de los procesos de negocio.
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.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					final.	la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					BAI10 Gestionar la Configuración.	Definir y mantener registros y relaciones entre los principales

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						recursos y capacidades necesarios para la prestación de servicios.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
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.	APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
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.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
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.	BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.01 Proteger contra software malicioso (malware).	Actividades de control contra software malicioso.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
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.	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
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.	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y	APO11.04 Supervisar	Actividades para planear y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Auditoría.	y hacer controles y revisiones de calidad.	monitorear los controles de calidad implementados.
					DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.
					APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						dentro de la organización.
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.	BAI10 Gestionar la Configuración	Definir y mantener registros y relaciones entre los principales recursos y capacidades necesarios para la prestación de servicios.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y el acceso lógico.	de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el		Art. 62	Paso 8. Revisiones y Auditoría.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
					APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					de la información y asociados con los requerimientos de la empresa.
					BAI03.10 Mantener soluciones.	Criterios para desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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.	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

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.	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
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.	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS03.02 Investigar y diagnosticar problemas.	Criterios para el proceso de investigación y diagnóstico de problemas.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las 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.		Art. 50	1. Recomendación General.	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.
					APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	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.				Servicios de Seguridad.	procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
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.	APO07.01 Mantener la dotación de personal suficiente y adecuado.	Criterios para mantener solo a personal necesario de acuerdo a las necesidades del negocio.
					APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de	APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
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:		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.	Criterios para la identificación y categorización de proveedores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Medidas de Seguridad.	APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
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		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO10.01 Identificar y	Criterios para la identificación y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	evaluar las relaciones y contratos con proveedores.	categorización de proveedores.
					APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas 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.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y el acceso lógico.	de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
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	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

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.				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
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.	APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la	Criterios para que los usuarios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					identidad del usuario y el acceso lógico.	tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.