Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales

Junio 2015

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Contenido

Notas de versiones

- Versión Noviembre 2014. Respecto a la versión anterior (Marzo 2014), se actualizó el *Paso 4. Elaborar un Inventario de Datos Personales*, para detallar la categorización de los sistemas de tratamiento de datos personales, en función de su nivel de riesgo inherente.
- Versión Junio 2015. Respecto a la versión anterior (Noviembre 2014), se actualizó el nombre, logotipo y sigla del Instituto, debido al cambio de naturaleza jurídica del antes Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), por el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

1. PRESENTACIÓN

En las Recomendaciones en materia de Seguridad de Datos Personales,[1] publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013, este Instituto recomendó la implementación de un **Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar),** para la protección de los datos personales.

En la presente guía, se brinda orientación para la implementación de un SGSDP con base en los siguientes estándares internacionales:

- BS 10012:2009 Data protection – Specification for a personal information management system
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.
- ISO/IEC 27005:2008, Information Technology–Security techniques– Information security risk management.
- ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework
- ISO 31000:2009, Risk management – Principles and guidelines
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards
- ISO GUIDE 73, Risk management – Vocabulary
- ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

De ese modo, se considera que las medidas de seguridad que se definan a partir de las referencias anteriores, y que se implementen de manera adecuada, permitirán que se cumpla con lo dispuesto por el Capítulo III del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, la Ley o LFPDPPP).

Con objeto de facilitar el análisis de las normas y estándares anteriores, el INAI ofrece, a través del presente documento, un ejercicio de concreción, síntesis y armonización de dichas referencias. En ese sentido, los responsables y encargados, así como todo interesado, encontrará en esta guía los pasos claves para realizar un SGSDP basado en el ciclo PHVA.

Importante

El objetivo general de este documento es orientar a los responsables y encargados para crear un **SGSDP, de manera que a través de un proceso de mejora continua se logre un nivel aceptable del riesgo en el tratamiento de la información personal, de acuerdo al modelo y objetivos de la organización.**

[1] Recomendaciones en materia de Seguridad de Datos Personales en: http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

Es importante que se tome en cuenta que el alcance del SGSDP **es la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas**. Por lo cual, el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de la presente guía se deberán enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones descritas en el artículo 63 del reglamento.

Esta guía se basa en la seguridad a través de la gestión del riesgo de los datos personales, entendiéndose de forma general al riesgo como una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Es importante señalar que la adopción de lo establecido en la presente guía es de carácter voluntario, por lo que los responsables y encargados podrán decidir libremente qué metodología conviene más aplicar en su negocio para la seguridad de los datos personales. Asimismo, el seguimiento de la presente guía no exime a los responsables y encargados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos ya que la seguridad de dichas bases depende de una correcta implementación de las medidas o controles de seguridad.

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

2.1 Definiciones

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Alta Dirección. Toda persona con poder legal de toma de decisión en las políticas de la organización. Por ejemplo: la junta directiva, ejecutivos y trabajadores experimentados, la persona a cargo del departamento de datos personales, los socios de la organización, el dueño de una empresa unipersonal o quien encabeza la organización.

Bases de datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

Custodios. Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.

Datos personales. Cualquier información concerniente a una persona física identificada o identificable.

Encargado. La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Impacto. Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Incidente. Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Amenaza. Circunstancia o evento con la capacidad de causar daño a una organización.

Vulnerabilidad. Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Organización. Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Parte interesada. Persona o grupo de personas con intereses específicos sobre una organización. Por ejemplo: inversionistas, clientes, proveedores, autoridades de protección de datos y titulares.

Responsable. Persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad. Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Identificar el riesgo. Proceso para encontrar, enlistar y describir los elementos del riesgo.

Valorar el riesgo. Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Comunicar el riesgo. Compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo.

Tratar el riesgo: Procesos que se realizan para modificar el nivel de riesgo.

Aceptar el riesgo. Decisión informada para coexistir con un nivel de riesgo.

Compartir el riesgo. Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

Evitar el riesgo. Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

Reducir el riesgo. Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

Retención del riesgo. Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

Riesgo residual. El riesgo remanente después de tratar el riesgo.

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Confidencialidad. Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

Disponibilidad. Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

Integridad. La propiedad de salvaguardar la exactitud y completitud de los activos.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Titular. La persona física a quien corresponden los datos personales.

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia. Toda comunicación de datos realizada a persona distinta del titular, responsable o encargado del tratamiento, dentro o fuera del territorio nacional.

2.2 ¿Qué es un Sistema de Gestión?

La **gestión** es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea. Un **sistema** es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un **Sistema de Gestión (SG)** se define como un conjunto de elementos y actividades interrelacionadas para establecer **metas** y los **medios de acción** para alcanzarlas.

Asimismo, un sistema de gestión apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de la organización, mediante la consideración de las necesidades de todas las partes interesadas.

Es importante tomar en cuenta que una organización tiene que definir y gestionar numerosas actividades para funcionar con eficiencia. Estas actividades se convierten en procesos que tienen la característica de recibir elementos de entrada, los cuales se gestionan para regresar al final de su ciclo, como elementos de salida (resultados). Por ejemplo, un proceso de Auditoría puede recibir como elementos de entrada objetivo, alcance y plan de auditoría, así como el informe de resultados de la auditoría anterior, y como elemento de salida un nuevo informe de auditoría. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente, y la interconexión entre procesos genera sistemas que se retroalimentan para mejorar.

En el caso de las Recomendaciones en materia de Seguridad de los Datos Personales, emitidas por el INAI, el sistema de gestión propuesto se basa en el modelo denominado "Planificar-Hacer-Verificar-Actuar" (PHVA), a través del cual se dirigen y controlan los procesos o tareas, como se puede ver en la tabla 1 y figura 1:

	Elemento del SG	Fase del PHVA	Actividades
PROCESO	**Metas**	**P**lanificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta).
	Medios de acción	**H**acer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras informaciones relevantes, para lograr la mejora continua.

Tabla 1. Sistema de Gestión

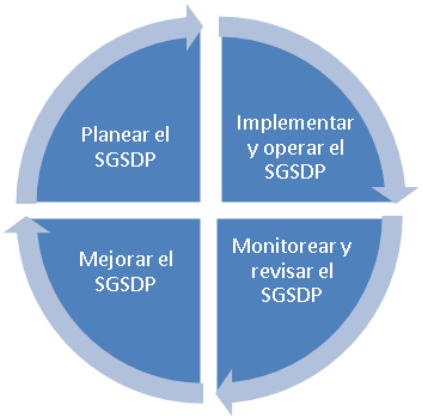

Figura 1. Ciclo General del Sistema de Gestión de Seguridad de Datos Personales

2.3 Introducción al Sistema de Gestión de Seguridad de Datos Personales

En particular, el SGSDP tiene como objetivo proveer un marco de trabajo para el tratamiento de datos personales que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas.

Las fases del ciclo PHVA considera diferentes pasos y objetivos específicos para el SGSDP, que pueden observarse en la siguiente tabla:

	Fases		Pasos	Objetivos Específicos
Ciclo	Planificar	Planear el SGSDP	1. Alcance y objetivos 2. Política de gestión de datos personales 3. Funciones y obligaciones de quienes traten datos personales 4. Inventario de datos personales 5. Análisis de riesgos de los datos personales 6. Identificación de las medidas de seguridad y análisis de brecha	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para **gestionar los riesgos de los datos personales**, con el fin de **cumplir con la legislación sobre protección de datos** y obtener resultados acordes con las políticas y objetivos generales de la organización.
	Hacer	Implementar y operar el SGSDP	7. Implementación de las medidas de seguridad aplicables a los datos personales	Implementar y operar las políticas, objetivos, procesos y procedimientos del SGSDP, así como sus controles o mecanismos con indicadores de medición.
	Verificar	Monitorear y revisar el SGSDP	8. Revisiones y auditoría	Evaluar y medir el cumplimiento del proceso de acuerdo con la **legislación de protección de datos personales**, la política, los objetivos y la experiencia práctica del SGSDP, e informar los

			resultados a la Alta Dirección para su revisión.
Actuar	Mejorar el SGSDP	9. Mejora continua y Capacitación	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte de la Alta Dirección, las auditorías al SGSDP y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

Tabla 2. Objetivos del SGSDP dentro de las fases del ciclo PHVA

La mayoría de las organizaciones poseen de manera consciente o no, de manera documentada o no, uno o más procesos que involucran el tratamiento de datos personales; estos procesos deben ser identificados y controlados a partir de que la información es recolectada y hasta que se bloquea, se borra o se destruye.

Más aún, en el marco de la Ley y su Reglamento, los datos personales son el principal activo de información. En consecuencia, a través del artículo 61 del Reglamento se puede vislumbrar que una de las primeras acciones para llevar a cabo su protección es tener bien identificado, definido y documentado el flujo de los datos personales que se traten a través de los diferentes procesos de la organización.

Asimismo, durante el ciclo del SGSDP se deben identificar los riesgos relacionados a los datos personales, así como al resto de activos que interactúan directamente con ellos, y de ese modo determinar los controles de seguridad que pueden mitigar los incidentes.

En la siguiente sección se detallarán las acciones que se recomiendan llevar a cabo para la seguridad de los datos personales, basadas en el ciclo PHVA, considerando que cada uno de los pasos del SGSDP debe mantener un adecuado registro documental.

3. Acciones para la Seguridad de los Datos Personales

Fase 1. Planear el SGSDP

Como se señaló anteriormente, en la fase de **planeación** del SGSDP se requiere establecer los objetivos y procesos necesarios para llegar a la meta u obtener los resultados esperados por la organización, en este caso en particular, la protección y seguridad de los datos personales. Para ello, es necesario realizar, al menos, las siguientes acciones, que se detallarán a continuación:

1. Establecer el **alcance y los objetivos** de la gestión de los datos personales;
2. Elaborar una **política de gestión** de datos personales;
3. **Establecer las funciones y obligaciones de quienes traten los datos personales;**
4. **Elaborar un inventario de datos personales**;
5. Analizar los riesgos a los que están sujetos los datos personales, y
6. Identificar las medidas de seguridad y realizar el análisis de brecha.

Paso 1. Establecer el Alcance y los Objetivos

El responsable debe definir el alcance y establecer los objetivos del sistema de gestión. Es decir a partir del contexto general de la información y los procesos que posee la Organización, se debe delimitar el ámbito de aplicación que involucra el tratamiento relacionado con el flujo de los datos personales, considerando:

a) De dónde se obtienen los datos personales (directamente del titular, a través de una transferencia o fuente de acceso público, entre otros);
b) Las unidades de negocio o, departamentos que tratan datos personales para los servicios que ofrecen o actividades que realizan;
c) En particular, qué empleados o miembros de la organización están autorizados a tratar los datos personales;
d) Las finalidades del tratamiento;
e) Con quién se comparten los datos personales (encargados o transferencias) y para qué se comparten;
f) En dónde y cómo se almacenan los datos personales;
g) Los procedimientos, mecanismos y tecnología utilizados para el tratamiento;
h) Cuánto tiempo se conservan los datos personales, y
i) Los procedimientos para su destrucción

Así como, los estatutos aplicables, regulatorios y contractuales; las obligaciones organizacionales, las necesidades de las partes interesadas y el nivel de aceptación del riesgo, en caso de que exista para la organización.

Por otra parte, el responsable deberá considerar entre los objetivos del SGSDP aquéllos que permitan el tratamiento legítimo, controlado e informado de los datos personales, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (derecho que tienen los individuos de decidir a quién y para qué proporcionan su información personal). Los objetivos deben ser expresados generalmente como metas medibles. Por ejemplo, reducir el número de vulneraciones a los datos personales.

Para determinar el objetivo del SGSDP, se sugiere al responsable tomar en cuenta los siguientes factores:

Factores contractuales: Estas obligaciones surgen de los acuerdos existentes entre los diferentes actores del tratamiento de datos personales y sus interacciones, en función del flujo de la información.

Escenarios	TITULAR	RESPONSABLE	ENCARGADO	TERCERO
a)	Entrega DP	Recibe DP	-	-
b)	-	Entrega DP	Recibe DP	-
c)	Entrega DP	-	Recibe DP	-
d)	Recibe DP	Entrega DP	-	-
e)	Recibe DP	-	Entrega DP	-
f)	-	Recibe DP	Entrega DP	-
g)	-	Entrega DP	-	Recibe DP
h)	-	-	Entrega DP	Recibe DP

Tabla 3 Tabla de factores contractuales para definir objetivos en la organización

Como puede observarse en la Tabla 3, donde DP representa Datos Personales, cada escenario de flujo de información tiene diferentes implicaciones contractuales y legales:

a) El **Titular** entrega DP al **Responsable.** Por ejemplo, cuando una persona se registra para recibir un servicio.
b) El **Responsable** entrega DP al **Encargado**. Por ejemplo, cuando el **Encargado** realiza un tratamiento de DP como parte de un contrato de servicio.
c) El **Titular** entrega DP al **Encargado.** Por ejemplo, un titular atendido por un Call-Center contratado por el Responsable.
d) El **Titular** recibe DP a través del ejercicio de sus derechos ARCO directamente con el **Responsable**.
e) El **Titular** recibe DP a través del ejercicio de derechos ARCO por medio del **Encargado** que actúa en representación del Responsable.
f) El **Encargado** entrega DP al **Responsable**. Por ejemplo, por terminación de contrato de servicios y migración de datos personales con otro proveedor.
g) El **Responsable** entrega DP a un **Tercero**. Por ejemplo, a través de una transferencia por un acuerdo de colaboración comercial.
h) El **Encargado** entrega DP a un **Tercero**. Por ejemplo, por una instrucción del responsable.

Factores legales y regulatorios: se reflejan en leyes nacionales y locales o acuerdos internacionales, así como en la regulación secundaria. Por ejemplo la LFPDPPP y su Reglamento, leyes de protección al consumidor, leyes de notificación de vulneraciones, leyes laborales, entre otras.

Factores del modelo de negocio: Se basan en las características específicas del modelo de negocio, por lo que varían de una organización a otra. Por ejemplo, los factores de negocio podrían estar alineados a guías, códigos de conducta o mejores prácticas de un sector específico.

Factores tecnológicos: Se basa en el entendimiento de la organización respecto a las tecnologías que se utilizan para tratar datos personales, su grado de madurez en su modelo de negocio, así como su experiencia en manejo de las tecnologías.

Paso 2. Elaborar una Política de Gestión de Datos Personales

Una vez que han sido definidos los alcances y objetivos de la gestión de los datos personales, el responsable directamente, o bien un equipo de la Alta Dirección autorizado por él, deberá emitir e implementar una política de gestión y seguridad que ayude al logro de los objetivos planteados. Además, es fundamental darle seguimiento a la política, mantener su implementación a través del tiempo y actualizar o realizar ajustes a la misma cuando sea necesario. Asimismo, en función del tamaño y necesidades de la organización, se podrían generar equipos de trabajo adicionales para desarrollar tareas específicas como la identificación de activos, procesos, funciones y responsabilidades.

La política debe tener muy bien definidos su alcance y objetivo, y recordar que aplica a todos los datos personales que son tratados en la organización dentro de los distintos procesos y finalidades convenidas con los titulares. Dicha política debe ser formalmente aprobada y apoyada por la Alta Dirección.

La política debe establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento, por lo que debe ser comunicada a los mismos, e incluir al menos las siguientes reglas:

a) El cumplimiento de todos los principios que establece el artículo 6 de la Ley: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, conforme a lo que señala la propia Ley, su Reglamento y demás normativa aplicable;
b) Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud);
c) Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento);
d) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información);
e) Procurar que los datos personales tratados sean correctos y actualizados (principio de calidad);
f) Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron (principio de calidad);
g) Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad);
h) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad);
i) No obtener los datos personales a través de medios fraudulentos (principio de lealtad);
j) Respetar la expectativa razonable de privacidad del titular (principio de lealtad);
k) Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad);
l) Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad);
m) Establecer y mantener medidas de seguridad (deber de seguridad);
n) Guardar la confidencialidad de los datos personales (deber de confidencialidad);
o) Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen;
p) Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la organización;
q) Respetar los derechos de los titulares en relación con su datos personales;
r) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;
s) Desarrollar e implementar un SGSDP de acuerdo a la política de gestión de datos personales, y
t) Definir las partes interesadas y miembros de la organización con responsabilidades específicas y a cargo de la rendición de cuentas para el SGSDP.

Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales

El responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el SGSDP. Para asegurar que la gestión de los datos personales sea parte de los valores de la organización de manera efectiva, el responsable debe:

a) Comunicar a todos los involucrados en el tratamiento de los datos personales (internos y externos) la importancia de:
   - cumplir la política de gestión de datos personales;
   - conocer los objetivos del SGSDP, y
   - mejorar el SGSDP de manera continua;

b) Definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional para el SGSDP, y

c) Asegurar que todos los trabajadores tengan claro sus roles y funciones (ver Tabla 4), así como su contribución para el logro de los objetivos del SGSDP de la organización y las consecuencias del incumplimiento.

Actividades	Área de la Organización							
	Dirección y Gestión	Finanzas y Contabilidad	Recursos Humanos	TIC	Área Legal	Auditoría Interna	Terceros	Infraestructura
Política y Objetivos del SGPDP	●	●	●	●	●			
Funciones y Obligaciones de Quienes Traten Datos Personales	●	●	●	●	●	●	●	●
Inventario de Datos Personales	●	●	●	●		●	●	●
Análisis de Riesgo de los Datos Personales	●	●	●	●	●	●	●	●
Análisis de Brecha de las Medidas de Seguridad		●	●	●	●	●	●	●
Implementación de las Medidas de Seguridad Aplicables a los Datos Personales	●	●	●	●	●	●	●	●
Revisiones y Auditoría						●		
Capacitación	●	●	●	●	●	●	●	●

Tabla 4. Ejemplo de esquema de contribuciones al SGSDP por área dentro de la organización

Paso 4. Elaborar un Inventario de Datos Personales

Se debe establecer y mantener actualizado un inventario de los sistemas de tratamiento de datos personales que utiliza una organización. Este inventario debe identificar o estar vinculado con la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su flujo o ciclo de vida, considerando:

- Obtención;
- Almacenamiento
- Uso:
  - Acceso
  - Manejo
  - Aprovechamiento

    - Monitoreo
    - Procesamiento (incluidos los sistemas que se utilizan para tal fin)
- Divulgación:
    - Remisiones
    - Transferencias
- Bloqueo;
- Cancelación, supresión o destrucción.

Figura 2. Tratamiento de datos personales

Por otra parte, es importante que el responsable tome en cuenta el riesgo inherente de los datos personales en los sistemas de tratamiento, es decir, el valor significativo tanto para los titulares y responsables, como para cualquier persona no autorizada que pudiera beneficiarse de ellos.

A continuación se ofrecen ejemplos de categorías para los sistemas de tratamiento de datos personales según su riesgo inherente:

a) Nivel estándar

Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

b) Nivel sensible

Esta categoría contempla los datos que permiten conocer la *ubicación física* de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país.

También son datos de nivel sensible aquéllos que permitan inferir el *patrimonio* de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el *número de tarjeta bancaria de crédito* y*/o débito.*

Son considerados también los datos de *autenticación* con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos *jurídicos* tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

c) Nivel especial

Esta categoría corresponde a los datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a los titulares, por ejemplo la *Información adicional de tarjeta bancaria* que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

La Tabla 5 contiene la clasificación por nivel de algunos tipos de dato:

Tipo de sistema de tratamiento de datos personales	Nivel
Información adicional al número de tarjeta bancaria	***Especial***
Ubicación física	***Sensible***
Patrimonio	***Sensible***
Autenticación	***Sensible***
Jurídicos	***Sensible***
Salud, creencias, opiniones políticas	***Sensible***
Identificación y contacto	*Estándar*

Tabla 5. Ejemplos de categorización por tipo de dato

El riesgo inherente en los sistemas de tratamiento de datos personales puede incrementarse cuando se manejan grandes volúmenes de información personal, cuando se relacionan distintos tipos de datos o se combinan bases de datos de diferentes fuentes (cruces de información).

El nivel de riesgo en los sistemas de tratamiento de datos personales puede disminuirse con mecanismos como:

Disociación: *se aíslan los datos de manera que por sí mismos no aporten información valiosa de un titular o éste no pueda ser identificable. De esta manera el valor de la base de datos para una persona no autorizada se ve disminuido.*

Separación*: se separan los activos de información grandes en otros más pequeños, por ejemplo, una base de datos de clientes en dos bases de datos: clientes corporativos y personas físicas. Entre mayor cantidad de información tiene un activo, éste resulta más atractivo para una persona no autorizada.*

Las categorías para los sistemas de tratamiento antes descritas son sólo una orientación, ya que el Pleno del INAI no ha emitido criterios institucionales al respecto, además es importante remarcar que ciertos datos personales que en principio no se consideran sensibles, podrían llegar a serlo dependiendo del contexto en que se trate la información.

Una vez que se han identificado las categorías de los sistemas de tratamiento de datos personales, se tiene que definir su relación con el personal de la organización. Es decir, considerando la figura 2 se debe identificar qué tipo de tratamiento efectúa cada uno de ellos, así como el grado de responsabilidad, de modo que a través de un registro documentado se puedan conocer los privilegios y límites que tiene cada individuo. Esto ayuda a las organizaciones a ponderar, por ejemplo, aquellas áreas que necesitan controles de seguridad o entrenamiento más específico. En caso de una solicitud de derechos ARCO o una vulneración a la seguridad, es de utilidad tener identificado quiénes dentro de la organización puede ayudar con estos procesos.

Para documentar el cruce de información entre los sistemas de tratamiento y el personal involucrado, se podría utilizar una matriz de responsabilidades o un formato similar, como el mostrado en la Tabla 6.

Personal Relacionado	**Sistema de Tratamiento**		
	Base de datos Clientes	*Base de datos Prospectos*	*Base de datos Empleados*
Empleado A	OA		U
Empleado B	OA		U
Departamento M		OAUB	
Área X			BC

O - Obtención, U - Uso, D- Divulgación, A - Almacenamiento, B - Bloqueo, C - Cancelación

Tabla 6. Ejemplo de esquema de privilegio sobre el tratamiento

En el ejemplo se puede ver cómo el **Empleado A** puede obtener (**O**) y almacenar (**A**) datos para la *Base de datos de Clientes* y usar (**U**) los datos en la *Base de datos de Empleados*, sin embargo no tiene permisos sobre la *Base de datos Prospectos*. Por su parte los empleados del **Departamento M** pueden obtener (**O**), almacenar (**A**), usar (**U**) y bloquear (**B**) datos de la *Base de datos de Prospectos,* pero no tiene privilegios sobre alguna de las otras dos bases de datos.

Paso 5. Realizar el Análisis de Riesgo de los Datos Personales

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

El objetivo de esta sección es que los responsables determinen las características del riesgo que mayor impacto puede tener sobre los datos personales que tratan, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar.

Factores para Determinar las Medidas de Seguridad

Artículo 60 del Reglamento de la LFPDPPP:

"El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:
I. El riesgo inherente por tipo de dato personal;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico, y
IV. Las posibles consecuencias de una vulneración para los titulares.
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."

Para poder definir un plan del riesgo a tratar y posteriormente implementar controles de seguridad, se deben tener diferentes criterios de evaluación dentro de la organización, que permitan delimitar el **nivel de riesgo aceptable** para los datos personales. Estos **criterios de evaluación del riesgo** de la seguridad de los datos personales deben considerar los factores establecidos en el **artículo 60 del Reglamento** y de manera adicional, entre otros factores que pueden incidir en el nivel de riesgo se encuentran los siguientes:

- Los requerimientos regulatorios y obligaciones contractuales que se usaron para definir los objetivos y alcances.
- El valor de los datos personales, de acuerdo a su clasificación por tipo definida previamente y su flujo.
- El valor y exposición de los activos involucrados con los datos personales.
- Expectativas de las partes interesadas, así como las consecuencias negativas a la reputación de la organización, que pudieran derivar de una vulneración.

Considerando los factores anteriores, las organizaciones pueden establecer dos tipos de criterios de evaluación del riesgo, los de impacto y los de aceptación. Los primeros corresponden a todo el posible daño a los titulares, mientras que los de aceptación se alinean de manera general a los niveles de riesgo que una organización se fije como meta respecto a sus alcances y objetivos, estos criterios se detallan a continuación:

Criterios de impacto. Se definen en términos del posible nivel de daño y perjuicio al titular causado por un *evento negativo* a la seguridad de los datos personales, considerando:

- El valor de los datos para la organización
- El incumplimiento con las obligaciones legales y contractuales relacionadas con el titular
- Vulneraciones de seguridad (art. 63 del reglamento)
- Daño a la integridad de los titulares de datos personales
- Daño a la reputación de la organización

Criterios de aceptación del riesgo. La organización podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad sean consideradas como muy poco significativas. Estos criterios dependen de las políticas y objetivos de la organización y de las partes interesadas, considerando que:

- Se debe expresar el beneficio o el riesgo estimado para la organización, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo, riesgos que pueden resultar del incumplimiento a la Ley que no pueden ser aceptados.
- Se deben incluir múltiples umbrales, correspondientes a diferentes niveles de aceptación, previendo que los responsables acepten riesgos sobre esos niveles en circunstancias específicas.
- Los criterios de aceptación del riesgo pueden incluir requerimientos para una gestión futura, por ejemplo, un riesgo puede ser aceptado si hay aprobación y el compromiso de la Alta Dirección para tomar acciones que permitan reducirlo a un nivel aceptable dentro de un periodo definido más adelante.
- Para definir todo criterio de aceptación del riesgo es importante considerar:
    - Política(s) de la organización respecto al tratamiento de datos personales
    - Aspectos legales y regulatorios
    - Operaciones
    - Tecnología
    - Finanzas
    - Factores sociales y humanitarios

Estos criterios deberían estar formalmente documentados y ser utilizados como directriz para valorar el riesgo.

Valoración Respecto al Riesgo

Cuando se tienen definidos criterios de evaluación del riesgo, por ejemplo ¿cuál sería el riesgo estimado para la organización de no poner el aviso de privacidad a disposición de sus clientes? o ¿qué personas se verían afectadas y de qué forma si se sustrajera la base de datos con la nómina de la organización? Se tiene que valorar el riesgo de forma cuantitativa, cualitativa o ambas, para atenderlo en la fase de implementación.

La valoración del riesgo identifica los activos existentes, las amenazas aplicables, y los escenarios de vulneración. Asimismo, determina las consecuencias potenciales y prioriza los riesgos derivados respecto al contexto de la organización y los criterios de evaluación del riesgo.

Esta valoración del riesgo debe considerar:

- El establecimiento y mantenimiento de criterios de aceptación de riesgos.

- La determinación de los criterios para evaluar los riesgos.
- Asegurar que las diferentes evaluaciones del riesgo generen resultados consistentes válidos y comparables.

Identificar Activos

Artículo 61 del Reglamento de la LFPDPPP:

"**IX.** Realizar un registro de los medios de almacenamiento de los datos personales."

Un activo es cualquier valor para la organización que requiera ser protegido. En términos del SGSDP estos activos deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Los activos se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo.

Se pueden identificar dos tipos de activos:

- **Activos de información**, corresponden a la esencia de la organización:
  - Información relativa a los datos personales
  - Información de procesos del negocio en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de los mismos
- **Activos de apoyo**, en los cuales residen los activos de información, como son:
  - Hardware
  - Software
  - Redes y Telecomunicaciones
  - Personal
  - Estructura organizacional
  - Infraestructura adicional

Debe mantenerse actualizado el inventario de activos, así como los medios de almacenamiento en que residen las bases de datos personales.

Después de identificar y describir los activos de información y de apoyo, se podrán encontrar sus vulnerabilidades y posibles amenazas. Además, es importante **definir al custodio del activo**, quien se quedará a cargo de proveer la adecuada rendición de cuentas de cada uno de ellos, señalando que el custodio del activo no podrá ejercer la propiedad de éste, pero tendrá responsabilidad sobre su mantenimiento y seguridad. En el **Anexo A** se incluyen ejemplos de los tipos de activos.

Identificar Amenazas

Una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas y además provenir de adentro o desde afuera de la organización. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Los custodios de los activos y sus usuarios pueden proporcionar asesoría para identificar y estimar las amenazas relacionadas, por ejemplo, del área de recursos humanos, de los administradores de

tecnologías y seguridad, profesionales en seguridad física, del departamento legal, externos como compañías de seguros, gobiernos y autoridades nacionales entre otras fuentes informativas de investigación. Los aspectos culturales también deben ser considerados dentro de las amenazas.

En el **Anexo B** se pueden consultar ejemplos de amenazas.

Identificar Vulnerabilidades

Las vulnerabilidades son debilidades en la seguridad de los activos y pueden ser identificadas en los siguientes ámbitos:

- Organizacionales
- De procesos y procedimientos
- De personal
- Del ambiente físico
- De la configuración de sistemas de información
- Del hardware, software o equipo de comunicación
- De la relación con prestadores de servicios
- De la relación con terceros

La presencia de vulnerabilidades no causa daño por sí misma, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien, cuando surja algún cambio. Por ejemplo, un equipo de cómputo o un archivero con información personal es vulnerable a inundaciones si se encuentra instalado en un sótano por el que pasan las tuberías del servicio de suministro de agua. De manera inversa, la amenaza de inundación se descarta si el equipo de cómputo o el archivero con datos personales se localiza en la parte más alta del edificio, lejos de tuberías de agua y de amenazas ambientales relacionadas.

Los controles usados incorrectamente o con una mala implementación son una causa de vulnerabilidades. Un control puede ser entonces efectivo o no efectivo dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que pueden ser usadas para otros propósitos distintos a los que se habían destinado originalmente. Deben considerarse vulnerabilidades y amenazas provenientes de diferentes fuentes, por ejemplo, la posibilidad de que un correo electrónico sea interceptado por un atacante o que un empleado envíe información confidencial a su cuenta personal.

En el **Anexo C** se pueden consultar ejemplos de vulnerabilidades asociadas a amenazas.

Identificar Escenarios de Vulneración y Consecuencias

Se deben identificar las consecuencias de las posibles vulneraciones contempladas en el artículo 63 del Reglamento.

Un escenario de vulneración proviene de una amenaza que explota cierta vulnerabilidad o conjunto de vulnerabilidades. El impacto se determina considerando el grado de daño en los activos o los cambios en el nivel de objetivos definidos por la organización, que pueden afectar a más de un activo total o parcialmente. Las consecuencias pueden ser de naturaleza temporal, por ejemplo, la caída del servicio o de naturaleza permanente, por ejemplo, la destrucción de información escrita en documentos.

La organización debe identificar las consecuencias de una posible vulneración considerando los criterios para la evaluación del riesgo establecidos previamente, de forma que pueda priorizar los riesgos identificados.

El análisis de riesgo deberá arrojar como resultado un valor del riesgo para cada uno de los activos identificados con respecto a cada una de las vulneraciones mencionadas en el artículo 63 de Reglamento, de forma que se identifiquen los escenarios que podrían llevar a cada uno de los activos a las posibles vulneraciones y se seleccionen los controles y medidas de seguridad que permitan tratar dichos riesgos.

Con el conocimiento de los activos de información y de los controles existentes se puede realizar una ponderación de los escenarios de riesgo más importantes, considerando que el riesgo es la combinación de los factores: amenaza, vulnerabilidad e impacto.

Por ejemplo, al considerar dos escenarios sobre activos:

Escenario 1. **Expediente de Paciente** (papel)
Escenario 2. **Expediente de Paciente** (electrónico)

Un hospital puede tener como control un sistema anti-incendio pero no tener un antivirus, esto afectaría de manera distinta a los activos y, por tanto, a la evaluación del riesgo:

Activo	Amenaza	Vulnerabilidad	Daño/Impacto	Potencial/Probabilidad
Expediente de Paciente **(electrónico)**	Virus	Computadoras sin antivirus	Borrado permanente de información	**Muy probable**
Expediente de Paciente **(papel)**	Incendio	Material susceptible al fuego	Pérdida definitiva de información	**Poco probable**

Tabla 7. Comparación de escenarios de riesgo

Como puede observarse en la Tabla 7, la falta de un antivirus hace muy probable que pueda ocurrir un daño permanente a los expedientes de pacientes electrónicos, mientras que la amenaza de incendio tiene menor importancia puesto que existe un control (sistema anti-incendio) para mitigar ese riesgo.

Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha

Con base en el análisis de riesgos se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas que permitan disminuir los riesgos, y podrán ser seleccionadas del listado mostrado en el **Anexo D.** Dichos controles de seguridad se han agrupado en 10 dominios principales que son:

1. Políticas del SGSDP
2. Cumplimiento legal
3. Estructura organizacional de la seguridad
4. Clasificación y acceso de los activos
5. Seguridad del personal
6. Seguridad física y ambiental
7. Gestión de comunicaciones y operaciones
8. Control de acceso

9. Desarrollo y mantenimiento de sistemas
10. Vulneraciones de seguridad

Los principios establecidos en el artículo 6 de la Ley pueden utilizarse como base para la selección de medidas de seguridad que estén alineadas a la protección de datos personales. En particular, se pueden tomar en cuenta los siguientes criterios para elegir las medidas de seguridad efectivas que:

- Protejan los datos personales contra daño, pérdida, destrucción o alteración.
- Eviten el uso, acceso o tratamiento no autorizado.
- Impidan la divulgación no autorizada de los datos personales.

Una vez identificados los activos y procesos relacionados a los datos personales, así como las amenazas, vulnerabilidades y escenarios de incidentes relacionados, se puede proceder al análisis de brecha de las medidas de seguridad.

El análisis de brecha consiste en identificar:

- Las medidas de seguridad existentes
- Las medidas de seguridad existentes que operan correctamente
- Las medidas de seguridad faltantes
- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

Es importante tener claro cuáles son los controles que ya están funcionando en una organización de manera efectiva, con su respectivo nivel de madurez, así como las medidas identificadas como faltantes, para constituir un programa de trabajo que refleje los recursos designados, los responsables, y las fechas compromiso para su implementación. De manera que se pueda medir la eficacia del SGSDP con respecto de los riesgos tratados.

La madurez de los controles puede ser identificada en uno de los siguientes niveles:

- **Documentado.** Se ha plasmado en un documento las características y objetivos del control, así como las medidas que soportan su cumplimiento.
- **Implementado.** El control ya se encuentra puesto en marcha a través de una o más medidas de seguridad.
- **Registros.** Se generan registros de la operación del control y de sus medidas de seguridad.
- **Monitoreo.** Se han establecido métricas que permiten dar seguimiento a la eficacia del control.
- **Indicadores Clave de Rendimiento** (*Key Performance Indicators, KPI*) e Informes. Se han identificado las métricas más significativas y son reportadas a las Partes Interesadas para la toma de decisiones.
- **Mejora continua.** Se toman las acciones necesarias para incrementar la eficacia de los controles con respecto al monitoreo realizado.
- **Automatizado.** El control requiere poca o nula interacción de una persona, en su operación, monitoreo o ajustes.

Fase 2. Implementar y Operar el SGSDP

Como se señaló anteriormente, en esta fase se implementan y operan las políticas, procesos, procedimientos y controles o mecanismos del SGSDP. En el caso que nos ocupa, en esta fase se deberán implementar las medidas de seguridad que hayan resultado aplicables según el análisis de riesgos realizado en la fase de planeación.

Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales

Cumplimiento Cotidiano de Medidas de Seguridad

La organización deberá considerar un conjunto de indicadores para identificar de manera oportuna, cualquier cambio en el contexto de la organización y así mantener una visión general de la imagen del riesgo, entre más pronto se realice esta detección, las partes interesadas podrán tomar decisiones más efectivas para proteger los datos personales.

La naturaleza de los indicadores puede variar dependiendo del tipo de activo. Por ejemplo, vigilar la actitud de un empleado inconforme o que se dejen documentos con información personal en las impresoras o fotocopiadoras. El monitoreo de estos indicadores conllevan una detección temprana de posibles amenazas, y así lograr una respuesta a incidentes efectiva.

Deberá designarse un miembro del equipo del responsable para la rendición de cuentas de la gestión de los datos personales dentro de la organización, de modo que tanto el cumplimiento de la legislación en protección de datos, como la política de gestión y seguridad de datos personales, puedan ser demostrados.

El responsable designado al interior de la organización para la protección de datos personales, en los términos del artículo 30 de la Ley, deberá estar a cargo del cumplimiento de la política en el día a día. Esta función debe tener, al menos, las siguientes responsabilidades:

a) compromiso total del cumplimiento de la política;
b) desarrollo y revisión de la política;
c) asegurar la implementación de la política;
d) revisiones de la gestión de la política;
e) entrenamiento y concienciación necesaria de la política;
f) aprobación de procedimientos donde sean tratados los datos personales, como:
    - la administración y comunicación de noticias de privacidad;
    - el manejo de solicitudes de los titulares;
    - la recolección y manipulación de datos personales;
    - manejo de quejas;
    - la gestión de incidentes de seguridad;
    - contratación de servicios externos y prestación;
g) enlace con las personas a cargo del manejo de riesgos y asuntos de seguridad dentro de la organización;
h) provisión de asesoramiento en asuntos ante el INAI y en relación con proyectos que involucren temas de seguridad de los datos personales, como puede ser compartirlos o transferirlos fuera de la organización;
i) interpretación de las exenciones aplicables al tratamiento de la datos personales;

j) asegurar que la organización tenga acceso a actualizaciones legislativas y a una orientación apropiada de acuerdo a la legislación en protección de datos;
k) revisar que el SGSDP refleje los cambios en legislación, práctica y tecnología a través una comunicación continua y proactiva del riesgo a las partes interesadas;
l) completar, emitir, y gestionar notificaciones ante el INAI y los titulares de datos personales cuando sea requerido según la normatividad aplicable; y
m) en su caso, implementar las prácticas relacionadas al tratamiento de datos personales marcadas por cualquier normativa de sector mandatorio o consultivo que aplique a la organización.

Cuando la organización posee múltiples departamentos o sistemas que procesan información personal, debería determinar si es apropiado establecer una red de representantes en protección de datos personales, los cuales:

a) representen departamentos o sistemas que sean reconocidos como relevantes, ya sea por el tipo de proceso o por el tipo de dato personal que manejan en relación con la gestión de información; y
b) ayudar a los trabajadores con las responsabilidades diarias para el cumplimiento de la política.

En otros casos, el responsable podría tomar la decisión de contratar los servicios de una persona física o moral, especialista en la materia para llevar a cabo las funciones o responsabilidades relacionadas con el SGSDP. No obstante, cabe señalar que el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o por aquéllos que haya comunicado a un encargado.

Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes

Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el plan de tratamiento del riesgo, tomando en cuenta la ponderación hecha en la valoración. Existen cuatro posibilidades comunes para tratar el riesgo: mitigar o reducir el riesgo, retener el riesgo, evitar el riesgo y compartir el riesgo. La Figura 3 ilustra el tratamiento del riesgo dentro del proceso de un SGSDP.

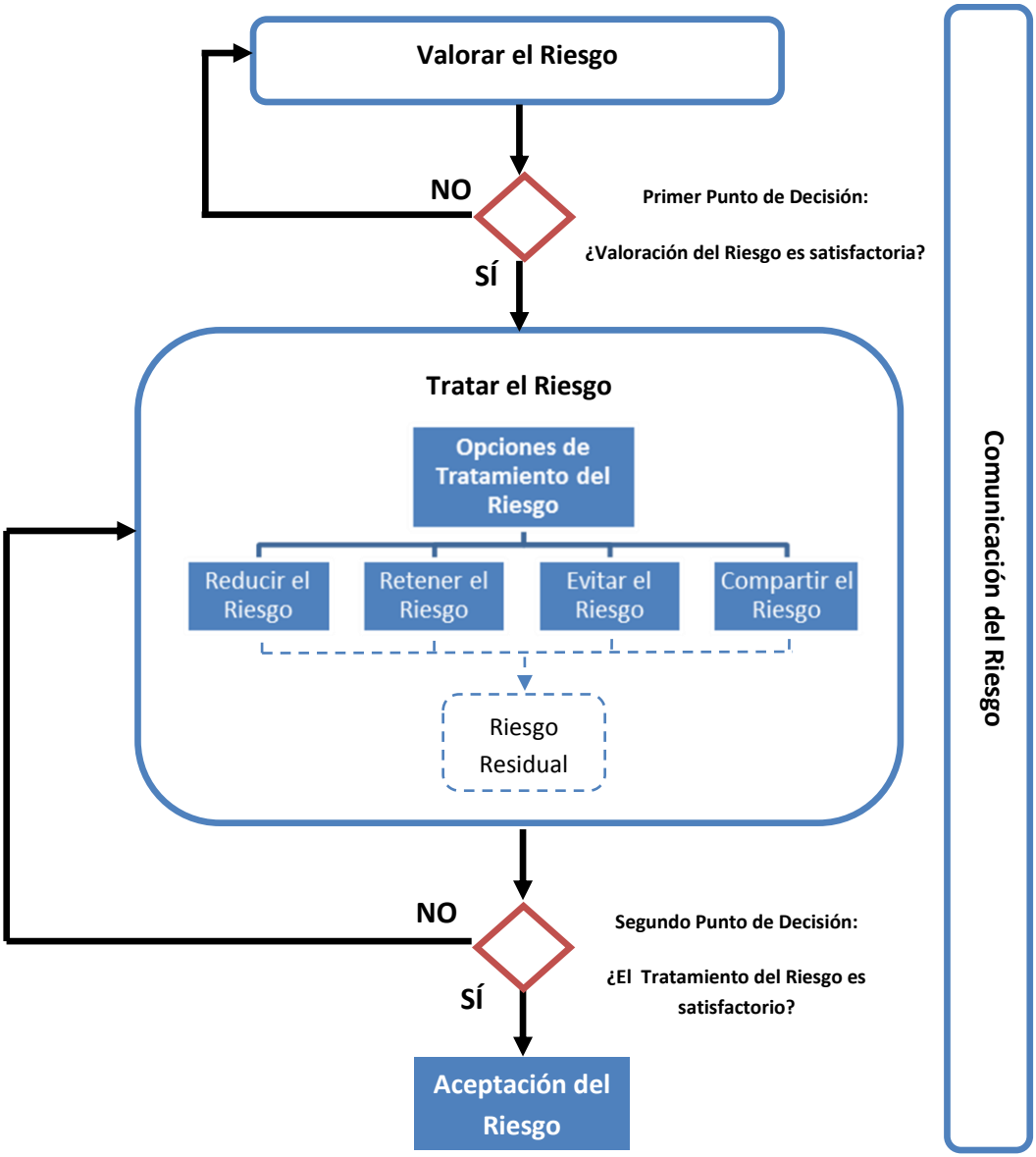

Figura 3. Tratamiento del Riesgo

Las opciones de tratamiento del riesgo deben ser seleccionadas con base en el resultado de la valoración del riesgo, los costos estimados, y los beneficios esperados de implementar estas opciones.

Si se obtiene una considerable reducción del riesgo con un costo relativamente bajo, esto es una combinación a considerar para implementar los controles. En general, las consecuencias adversas de los riesgos deben reducirse lo más razonablemente posible con independencia de cualquier criterio absoluto, por ejemplo, se deben considerar los riesgos que no ocurren con frecuencia pero que serían severos, en cuyo caso también se deben implementar controles.

Los cuatro tipos de tratamiento de riesgo no son mutuamente excluyentes, a veces las organizaciones pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual.

Algunos tratamientos pueden atender a más de un riesgo, por ejemplo, el entrenamiento y concienciación del personal. El plan de tratamiento del riesgo tiene que establecer prioridades de atención de riesgos específicos y su periodo, dicha prioridad puede establecerse equilibrando la valoración del riesgo y el análisis costo-beneficio de la implementación en relación con el presupuesto.

Una vez que se ha definido el plan de tratamiento, se requiere determinar el riesgo residual. Si el riesgo residual no cubre los niveles de aceptación de la organización, se deberá realizar otra iteración de tratamiento del riesgo antes de proceder a la aceptación del riesgo.

Finalmente se deben implementar los controles correspondientes así como documentar todas las acciones derivadas de la planeación e implementación del tratamiento del riesgo.

Opciones de Tratamiento de Riesgo

Reducir el Riesgo

El objetivo es seleccionar los controles apropiados y justificados para satisfacer los requerimientos especificados por la valoración del riesgo. Los controles pueden proporcionar uno o más de los siguientes tipos de protección:

- Corrección
- Eliminación
- Prevención
- Minimización del impacto
- Disuasión
- Recuperación
- Monitoreo
- Concienciación.

Durante la selección de controles es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles contra el valor del activo a proteger. Adicionalmente, se debe tener en consideración el conocimiento y habilidades especiales necesarias para definir e implementar nuevos controles o modificar los existentes.

Existen factores que pueden afectar la selección de controles. Límites técnicos, como requerimientos de rendimiento, capacidad de gestión (soporte operacional necesario) y los asuntos de compatibilidad, pueden obstaculizar el uso de ciertos controles o pueden inducir a errores humanos nulificando el control, dando un falso sentido de seguridad o incrementando el riesgo más allá del control, por ejemplo, exigir contraseñas complejas sin previo entrenamiento, llevando a los usuarios a escribir las contraseñas en papel. Los responsables deben identificar las soluciones que satisfagan sus requerimientos y que garanticen suficiente seguridad de los datos personales.

En el **Anexo D** se puede consultar un listado de controles comunes, así como su área de aplicación.

Retener el Riesgo

Se puede tomar la decisión de retener el riesgo sin considerar medidas adicionales si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente. Por ejemplo, el equipo

de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

Evitar el Riesgo
Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios, se debe tomar una decisión para evitar el riesgo, retirándose de las actividades actuales o cambiando las condiciones bajo las cuales operan dichas actividades. Por ejemplo, para un riesgo causado por la naturaleza podría ser más eficiente en costo mover físicamente el *site* de datos a una ubicación donde no exista el mismo riesgo o que se pueda mantener bajo control.

Compartir el Riesgo
Implica tomar la decisión de compartir el riesgo con un prestador de servicio que pueda gestionarlo, es decir, un tercero interviene para mitigar los posibles efectos de un riesgo por ejemplo, al contratar un seguro o un proveedor que administre la seguridad de la organización.
Cabe mencionar que cuando una organización comparte un riesgo no deja de ser responsable por la protección de los datos personales, además, es importante que se considere que involucrar a un nuevo actor en los procesos de la organización siempre representa un riesgo que debe ser analizado.

Un ejemplo de compartir riesgos asociados a la protección de datos personales es la adquisición de servicios del denominado cómputo en la nube, para lo cual deberá observarse lo establecido en el Artículo 52 del Reglamento.

No se debe confundir el concepto de Transferencia de datos personales con el de Compartir el Riesgo.

Artículo 67 del Reglamento de la LFPDPPP:

"La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado."

Si por ejemplo, una organización determina que su centro de datos es inseguro y decide contratar a un proveedor de cómputo en la nube para que ellos se encarguen de la gestión y seguridad de los datos personales, en este caso la relación contractual convierte al proveedor de computo en la nube en un Encargado que actúa sobre los datos a cuenta del Responsable, en tal caso se está compartiendo el riesgo sin que exista una transferencia de datos personales.

Cualquier transferencia de datos personales que no se sujete a las figuras de Responsable y Encargado deberá sujetarse a lo previsto por la Ley y su Reglamento.

Aceptación del Riesgo Residual
Al llegar al punto de aceptar el riesgo se deben asumir y registrar formalmente las decisiones sobre el plan de tratamiento del riesgo, así como el riesgo residual, el plan de tratamiento del riesgo debe describir cómo se tratarán los riesgos valorados para alcanzar los niveles de aceptación. Es importante que la Alta Dirección apruebe y revise tanto los planes de tratamiento, como el riesgo residual. Del mismo modo, deberá registrarse cualquier condición asociada con tal aprobación.

Aceptar el riesgo implica que **el riesgo residual no entre en conflicto con los criterios previamente establecidos en los objetivos y alcances de la organización**, por ejemplo, el riesgo residual no puede considerar la aceptación de un riesgo relacionado al cumplimiento de la LFPDPPP si ésta forma parte de las metas planteadas en el SGSDP.

Comunicación del Riesgo

Comunicar el riesgo es la actividad que resulta de alcanzar los acuerdos sobre el cómo administrar los riesgos, considerando su naturaleza, forma, probabilidad, severidad, tratamiento y aceptación.

La comunicación efectiva entre los involucrados es muy importante pues impacta en las decisiones que se deban tomar, de ahí que tendría que ser bidireccional para asegurar que los involucrados en la implementación del SGSDP y las partes interesadas entiendan los criterios en los que se basan las decisiones.

La comunicación del riesgo se debe realizar para alcanzar los siguientes objetivos:

- Ofrecer garantías sobre la gestión del riesgo
- Recolectar información sobre el riesgo
- Compartir los resultados de la valoración y el plan de tratamiento del riesgo
- Evitar o reducir las vulneraciones de seguridad por desconocimiento entre los involucrados en el SGSDP
- Dar soporte a la toma de decisiones
- Obtener nuevo conocimiento sobre la seguridad de la información
- Que los responsables de datos personales coordinen con los encargados y terceros, los planes de respuesta en caso de una vulneración
- Dar a los a los custodios y a las partes interesadas sentido de responsabilidad sobre el riesgo
- Incrementar la conciencia del riesgo en la organización

La organización debe desarrollar planes de comunicación del riesgo para las operaciones normales, así como para casos de emergencia, es decir, la comunicación del riesgo es una actividad continua.

Un método de comunicación entre los custodios y las partes interesadas es a través de comités para debatir acerca del riesgo, su tratamiento y aceptación, entre otros asuntos relacionados.

Es importante mantener la comunicación entre las áreas afines a la difusión y el departamento de datos personales para responder por ejemplo, a los particulares en caso de incidentes.

Artículo 64 del Reglamento de la LFPDPPP:

"El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes".

Fase 3. Monitorear y Revisar el SGSDP

En esta fase, como se señaló anteriormente, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.

Paso 8. Revisiones y Auditoría

Revisión de los Factores de Riesgo

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos del SGSDP de la organización y así mantener una visión general de la imagen del riesgo.

El riesgo no es estadístico: las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas. Por lo tanto, se requiere de constante monitoreo para detectar esos cambios, por ejemplo, se pueden apoyar de servicios externos que provean información respecto a las amenazas o vulnerabilidades.

Las organizaciones deben asegurar que los siguientes puntos estén continuamente monitoreados:

- Nuevos activos que se incluyan en los alcances de la gestión de riesgo.
- Modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
- Nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Incidentes y vulneraciones de seguridad.

Los factores que determinan la probabilidad de ocurrencia y consecuencias podrían cambiar, lo que afectaría la conveniencia y costos de las opciones de tratamiento. Los cambios mayores que afectan a la organización deben ser revisados de manera específica, no obstante que las actividades de monitoreo requieren de regularidad y periodicidad.

El resultado del monitoreo de riesgo puede afectar su tratamiento y aceptación, y en consecuencia el contexto que se establezca en la siguiente iteración del ciclo del SGSDP de la organización.

Auditoría

Se debe contar con un programa de auditoría interna para monitorear y revisar la eficacia y eficiencia del SGSDP. Este programa debe planearse, establecerse y mantenerse tomando en cuenta la política de gestión de datos personales. En su caso, se deben considerar auditorías a través de externos para procesos y circunstancias especiales, por ejemplo, cuando la organización desea unirse a un esquema de certificación.

Se deben establecer previamente los objetivos del programa de auditoría, el cual debe incluir el alcance e indicar explícitamente cualquier tratamiento de datos personales interno y externo a la organización, responsables, recursos, criterios a utilizar durante la auditoría, así como los procesos y/o áreas que serán auditadas.

La objetividad e imparcialidad del programa de auditoría debe ser asegurado por la apropiada selección de auditores y la conducción de la auditoría.

Las auditorías deben llevarse a cabo en intervalos de tiempo planeados para determinar si el SGSDP:

a) está operando de acuerdo con la política de gestión de datos personales y con los procedimientos establecidos, y
b) ha sido implementado y mantenido de acuerdo con los requerimientos tecnológicos.

Se debe proporcionar a la Alta Dirección los reportes de las auditorías sobre el SGSDP, detallando cualquier desviación significativa de la política de gestión de datos personales, como pueden ser asuntos relacionados con los procesos de seguridad que puedan afectar su cumplimiento.

La auditoría debe ofrecer al responsable información detallada respecto a cambios ocurridos en el SGSDP, además se debe realizar una auditoría inmediatamente después de la implementación de modificaciones mayores en el SGSDP o en los procesos críticos de la organización respecto al tratamiento de datos personales.

Como resultado de una auditoría se deben obtener observaciones sobre riesgos existentes para aplicar medidas preventivas, es decir, controles para que no ocurra una vulneración, así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

Vulneraciones a la Seguridad de la Información

Artículo 63 del Reglamento de la LFPDPPP:

"Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada".

Las revisiones y auditorías, así como diferentes indicadores y alertas en el SGSDP pueden avisar la ocurrencia de vulneraciones a la seguridad de los datos personales en cualquier fase del tratamiento.

La organización debe contar con procedimientos para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando al menos:

1) **Identificación de la vulneración.** En caso de un incidente de seguridad, la organización debe identificar:
    a. Los activos afectados junto con el personal a cargo
    b. Los titulares afectados
    c. Partes interesadas que requieran estar informadas y/o puedan tomar parte en la toma de decisiones para mitigar las consecuencias de la vulneración.

2) **Notificación de la vulneración.** Una vez identificada la vulneración, ésta se debe comunicar a los titulares de los datos personales para que puedan tomar medidas que mitiguen o eviten una posible afectación.

    Dependiendo del riesgo que implique para los titulares, la notificación de una vulneración puede ser a través de medios masivos como un anuncio en su página web, periódico, radio y televisión o bien, de manera personalizada.

Artículo 64 del Reglamento de la LFPDPPP:

"El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes".

La organización podría considerar notificar a las autoridades de protección de datos y/o impartición de justicia, entre otras partes interesadas que pudieran auxiliar en el proceso de mitigar el incidente. Además de la información pertinente sobre la vulneración, como puede ser la naturaleza del incidente y los datos personales comprometidos, se debe notificar de las acciones inmediatas que está tomando la organización, así como proporcionar mecanismos de atención para que los titulares estén informados y reciban recomendaciones para reducir su afectación.

Artículo 65 del Reglamento de la LFPDPPP:

"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, y
V. Los medios donde puede obtener más información al respecto".

3) **Remediación del incidente.** Una vez identificada la vulneración y después de haber realizado la respectiva notificación, se debe profundizar en el análisis de las causas del incidente para establecer medidas correctivas, las cuales incluyen medidas inmediatas para reducir los efectos de la vulneración, así como medidas a largo plazo por ejemplo, implementar controles técnicos o actualizar las políticas del SGSDP para evitar que incidentes similares o relacionados vuelvan a ocurrir.

Artículo 66 del Reglamento de la LFPDPPP:

"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".

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad al SGSDP deben estar debidamente documentados, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas con objeto de que la organización cuente con evidencia suficiente para mostrar al Instituto su diligencia en tomar las acciones necesarias para evitar o mitigar una vulneración a la seguridad de los datos personales, además de que estos procesos proporcionan información que sirve como entrada para los procesos de mejora continua del SGSDP.

Fase 4. Mejorar el SGSDP

Paso 9. Mejora Continua y Capacitación

En esta fase, se adoptan las medidas correctivas y preventivas en función de los resultados de la revisión o verificación efectuadas, o de otras informaciones relevantes, para lograr la mejora continua. Una parte fundamental de la fase de Mejora es la capacitación al personal.

Mejora Continua

El monitoreo de los factores de riesgo así como los resultados de las auditorías proporcionan información para demostrar la eficacia del SGSDP, pero también presentan las áreas de oportunidad donde éste puede ser mejorado. **Los puntos de mejora del SGSDP pueden corresponder a dos tipos:**

a) **Acciones correctivas.** Son las acciones encaminadas a eliminar las causas de fallas o incidentes **ocurridos** en el SGSDP, con objeto de prevenir que vuelvan a ocurrir, dichas acciones deben ser proporcionales a la gravedad del incidente.

   Las acciones correctivas deben atenderse considerando:

   i. El análisis y revisión de la falla o incidente;
   ii. Determinar las causas que dieron origen a la falla o incidente;
   iii. Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
   iv. Determinar e implementar las acciones necesarias;
   v. Registrar los resultados de las acciones tomadas;
   vi. Revisar la eficacia de las acciones correctivas tomadas.

b) **Acciones preventivas.** Son las acciones encaminadas a eliminar las causas de fallas o incidentes **posibles** en el SGSDP, dichas acciones deben ser proporcionales a las amenazas potenciales.

   Las acciones preventivas deben atenderse considerando:

   i. El análisis y revisión de la amenaza;
   ii. Determinar las fallas o incidentes que podría desencadenarse con una amenaza;
   iii. Evaluar las acciones necesarias para evitar que la falla o incidente ocurra;
   iv. Determinar e implementar las acciones necesarias;
   v. Registrar los resultados de las acciones tomadas;
   vi. Revisar la eficacia de las acciones preventivas tomadas.

La implementación de las acciones preventivas o correctivas puede establecerse en un periodo inmediato a la detección y análisis del punto de mejora (por ejemplo, en respuesta a los resultados de una auditoría de certificación) o calendarizarse para una futura revisión del SGSDP en función de la importancia de la mejora y los recursos disponibles. La eficacia de las acciones preventivas y correctivas se evalúa considerando la reducción de los niveles de riesgo en los resultados del monitoreo a los SGSDP o de auditorías posteriores.

En función de las acciones correctivas y preventivas, así como de la actualización del contexto de la organización resultado del monitoreo del riesgo, se deben establecer o mejorar los planes de capacitación.

Capacitación

La mejor medida de seguridad contra posibles vulneraciones es contar con personal consciente de sus responsabilidades y deberes respecto a la protección de datos personales y que identifiquen cuál es su contribución para el logro de los objetivos del SGSDP. Por ello, se deben establecer y mantener programas de capacitación que mantengan vigente al SGSDP como:

a) **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en la organización;
b) **Entrenamiento:** programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;
c) **Educación:** programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la organización.

Se debe realizar una detección de necesidades para identificar el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Estos programas de capacitación deben tomar en cuenta elementos como:

a) Requerimientos y actualizaciones al contexto del SGSDP, considerando principalmente;
   1. la administración y comunicación de noticias de privacidad;
   2. el manejo de solicitudes y quejas de los titulares;

3. la recolección y manipulación de datos personales;
4. la gestión de incidentes y vulneraciones de seguridad, y
5. la gestión de seguridad con terceros.

b) La legislación en protección de datos personales y mejores prácticas relacionadas al tratamiento de datos aplicables a la organización;
c) Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales;
d) Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad, y
e) Instructores expertos en la materia.

Finalmente se debe evaluar la eficiencia y eficacia de la capacitación, esta evaluación se puede llevar a cabo mediante la aplicación de exámenes teóricos o prácticos que permitan indicar el grado de conocimiento y/o entendimiento de la capacitación proporcionada o difusión realizada. Se deben establecer criterios de evaluación que determinen el nivel de competencia aceptado por la organización, y mantener un registro de los programas seguidos por cada empleado, así como de sus habilidades, experiencia y calificaciones.

4. SÍNTESIS DE LA IMPLEMENTACIÓN DEL SGSDP

En esta sección se presenta una síntesis de los pasos del proceso de implementación de un SGSDP, para que los responsables la usen como una referencia rápida del contenido total de este documento.

1. Presentación. Alcances y objetivos de la guía.

2. Sistema de Gestión de Seguridad de Datos Personales –SGSDP. Descripción del Sistema de Gestión y su relación con la Seguridad de los Datos Personales**.**

2.1 Definiciones

2.2 ¿Qué es un Sistema de Gestión?

2.3 Introducción al SGSDP

2.4 Acciones para la Seguridad de los Datos Personales. En esta sección se definen los pasos para la planeación, implementación, vigilancia y mejora de un SGSDP.

Fase 1. Planear el SGSDP

Paso 1. Alcance y Objetivos. Consideraciones respecto al tratamiento de datos personales y el modelo de negocios de la organización.

Paso 2. Política de Gestión de Datos Personales. El compromiso formal documentado de la Alta Gerencia hacia el tratamiento adecuado de datos personales en la organización.

Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales. Asignación de responsabilidades para la implementación del SGSDP.

Paso 4. Inventario de Datos Personales. Identificación de los tipos de datos y su flujo.

Paso 5. Análisis de Riesgo de los Datos Personales.

- **Factores para Determinar las Medidas de Seguridad.** Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.
- **Valoración Respecto al Riesgo.** Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional, se compone de los siguientes pasos:
  - **Identificar Activos**
  - **Identificar Amenazas**
  - **Identificar Vulnerabilidades**
  - **Identificar Escenarios de Vulneración y Consecuencias**

Paso 6. Identificación de las Medidas de Seguridad y Análisis de Brecha. Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener. Los controles de seguridad, sin que sean limitativos, deben considerar los siguientes dominios:

- Políticas del SGSDP

- Cumplimiento legal
- Estructura organizacional de la seguridad
- Clasificación y acceso de los activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Vulneraciones de seguridad

Fase 2. Implementar y Operar el SGSDP

Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.

- **Cumplimiento Cotidiano de Medidas de Seguridad.** Consideraciones para el trabajo cotidiano con datos personales así como el plan de tratamiento del riesgo de los activos relacionados a los mismos.
- **Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.** Proceso en el que se decide y se implementa el tratamiento adecuado para un riesgo o grupo de riesgos respecto al contexto de la organización, dicho tratamiento considera:
  - **Opciones de Tratamiento de Riesgo**
    - **Reducir el Riesgo**
    - **Retener el Riesgo**
    - **Evitar el Riesgo**
    - **Compartir el Riesgo**
  - **Aceptación del Riesgo Residual**
  - **Comunicación del Riesgo**

Fase 3. Monitorear y Revisar el SGSDP

Paso 8. Revisiones y Auditoría. Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP.

- **Revisión de los Factores de Riesgo.** Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP.
- **Auditoría.** Requerimientos para los procesos de auditoría interna/externa.
- **Vulneraciones a la Seguridad de la Información.** Consideraciones en caso de un incidente de seguridad como la identificación, notificación y remediación.

Fase 4. Mejorar el SGSP

Paso 9. Mejora Continua y Capacitación. Consideraciones para incluir la protección de datos en la cultura de la organización y mantener siempre actualizado el SGSDP.

- **Mejora Continua.** La aplicación de medidas preventivas y correctivas sobre el SGSDP.
- **Capacitación.** Programas de mejora en el personal para mantener la vigencia del SGSDP.

Tabla Comparativa entre el Capítulo III del Reglamento de la Ley y la Guía

Capítulo III De las Medidas de Seguridad en el Tratamiento de Datos Personales	Acción que ayuda a cumplir con la disposición
Alcance	
Artículo 57. El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales. Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.	Adopción de un SGSDP Paso 1. Alcance y Objetivos Paso 2. Política de Gestión de Datos Personales
Atenuación de Sanciones	
Artículo 58. En términos de lo dispuesto en el artículo 65, fracción III de la Ley, en los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar la atenuación de la sanción que corresponda.	Adopción de un SGSDP
Funciones de seguridad	
Artículo 59. Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales. Asignación de responsabilidades para la implementación del SGSDP. Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales • Cumplimiento Cotidiano de Medidas de Seguridad
Factores para determinar las medidas de seguridad	
Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: **Fracción** I El riesgo inherente por tipo de dato personal;	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales • Factores para Determinar las Medidas de Seguridad

Fracción II La sensibilidad de los datos personales tratados; **Fracción III**. El desarrollo tecnológico, y **Fracción IV.** Las posibles consecuencias de una vulneración para los titulares. 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.	
Acciones para la seguridad de los datos personales	
Artículo 61. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:	Adopción de un SGSDP
Fracción I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;	Paso 4. Elaborar un Inventario de Datos Personales
Fracción II. Determinar las funciones y obligaciones de las personas que traten datos personales;	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales
Fracción III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales**;**	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales
Fracción IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fracción V. 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;	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha
Fracción VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;	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
Fracción VII. Llevar a cabo revisiones o auditorías;	Paso 8. Revisiones y Auditoría
Fracción VIII. Capacitar al personal que efectúe el tratamiento, y	Paso 9. Mejora Continua y Capacitación • Capacitación

Fracción IX. Realizar un registro de los medios de almacenamiento de los datos personales.	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales
El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.	Acciones a implementar para la seguridad de los datos personales documentadas
Actualizaciones de las medidas de seguridad	
Artículo 62. Los responsables deberán actualizar la relación de las medidas de seguridad, cuando ocurran los siguientes eventos: **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 del presente Reglamento, o **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.	Paso 8. Revisiones y Auditoría.
Vulneraciones de seguridad	
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase de tratamiento son: **I.** La pérdida o destrucción no autorizada; **II.** El robo, extravío o copia no autorizada; **III.** El uso, acceso o tratamiento no autorizado, o **IV.** El daño, la alteración o modificación no autorizada.	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales
Notificación de vulneraciones de seguridad	
Artículo 64. El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.	Paso 8. Revisiones y Auditoría. • Vulneraciones a la Seguridad de la Información.

Información mínima al titular en caso de vulneraciones de seguridad	
Artículo 65. 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, y **V.** Los medios donde puede obtener más información al respecto.	Paso 8. Revisiones y Auditoría. • Vulneraciones a la Seguridad de la Información
Medidas correctivas en caso de vulneraciones de seguridad	
Artículo 66. 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.	Paso 9. Mejora Continua y Capacitación • Mejora Continua

Anexos

Anexo A. Ejemplos de Activos

En la siguiente tabla se muestran los principales tipos de activos que pueden ser considerados por los responsables (otros tipos de activos podrían surgir dependiendo del avance tecnológico, así como del contexto de la organización):

Tipo de Activo	Ejemplos
Activos de información	
Información	Información personal (datos personales) definida en el contexto de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Adicionalmente podría ser considerado lo dispuesto en la materia por acuerdos internacionales, normatividad específica de la industria, o del giro particular del negocio, entre otros.
	Información estratégica, de alto costo o vital para alcanzar los objetivos determinados en el SGSDP, relacionada con el tratamiento de los datos personales, o cuya pérdida, modificación o redistribución no autorizada afecte a la reputación o estado legal de la organización.
Conocimiento de procesos del negocio **Incluye subprocesos y actividades**	Procesos cuya modificación, pérdida o degradación evitarían cumplir con la política de protección de datos personales de la organización.
	Procesos que contienen tecnología propietaria para el tratamiento de datos personales.
	Procesos que son necesarios para cumplir con requerimientos contractuales, legales o regulatorios de la organización.
Activos de Apoyo	
Hardware **Consiste en todos los elementos físicos que soportan procesos de datos personales**	**Equipo de procesamiento de datos.** Equipo para el procesamiento automático de información personal, incluyendo los elementos que operan independientemente. Por ejemplo, servidores, estaciones de trabajo, computadoras de cualquier clase.
	Equipo móvil. Equipo de cómputo portátil. Por ejemplo laptops, tablas, smartphones.
	Periféricos. Equipo conectado a una computadora para la entrada, y salida de datos. Por ejemplo, impresora, mouse, teclado.

Tipo de Activo	Ejemplos
Soportes **Medios de almacenamiento de datos personales**	**Soportes electrónicos.** Medios electrónicos de información inteligibles mediante el uso de un dispositivo electrónico como una computadora, para examinar, modificar o almacenar los datos. Por ejemplo, discos ópticos (CD's yDVDs), cintas magnéticas de audio, video y datos, fichas de microfilm, discos duros removibles, memorias USB, y demás medios de almacenamiento masivo no volátil.
	Soportes físicos. Medios de información inteligibles a simple vista, que no requieren de ningún dispositivo electrónico que procese su contenido para examinar, modificar o almacenar los datos. Por ejemplo, papel escrito a mano o impreso, transparencias, fotografías, placas radiológicas, entre otros.
Software **Consiste en todos los programas y aplicaciones que contribuyen a al procesamiento de datos personales**	**Sistemas Operativos (SO).** Incluye a todos los programas que funcionan como plataforma base para que operen otros programas tales como servicios y aplicaciones. Los principales elementos de un SO son los relacionados a la gestión de servicios de equipo (CPU, memoria, discos, e interfaces de red), gestión de tareas o procesos, y servicios de gestión de permisos de usuario.
	Software de servicio, mantenimiento o administración del software. Este complementa los servicios del SO y no es directamente accesible por los usuarios o aplicaciones (incluso cuando es indispensable para la operación global de sistemas de información). Por ejemplo, plataformas de actualización, antivirus empresariales.
	Paquetería de software o software estándar. Son productos completamente comercializados que proveen servicios a los usuarios y aplicaciones, pero no están personalizados para requerimientos especiales de la organización como ocurriría con una aplicación de negocio. Por ejemplo administradores de bases de datos, mensajería instantánea, servidores web, editores de texto, etc.
	Aplicaciones de negocio. Su campo de acción es muy amplio, y variado. Se refiere a software comercial o diseñado *in-house* con el objetivo de ofrecer al usuario servicios y funciones específicas que apoyen en la operación del Sistema de Gestión de Datos Personales.
Redes y Telecomunicaciones **Consisten en todos los dispositivos usados para interconectar computadoras o elementos de un sistema de información de voz y/o datos**	**Medios y equipos.** Los medios y equipos de comunicaciones y telecomunicaciones están definidos principalmente por las características físicas y técnicas (punto-a-punto, broadcast) y por los protocolos de comunicación (protocolos de enlace, de red). Ejemplos: Red Telefónica Pública Conmutada, Ethernet, Especificaciones de protocolos wireless (por ejemplo, WiFi 802.11), Bluetooth, etc. También se deben considerar los elementos que dan soporte a los protocolos de comunicación de red, incluyen funciones de enrutamiento y/o filtrado de las comunicaciones (por ejemplo, bridge, router, switch, hub); las interfaces (físicas y lógicas) para conectar diferentes medios o protocolos; y los servicios y equipo de telecomunicaciones proporcionados por un operador (por ejemplo: líneas telefónicas externas e internas).
Sitio **Comprende todos los lugares o**	**Ambiente externo.** Se refiere a aquellos lugares que quedan fuera del alcance de la organización. Por ejemplo: vivienda del personal, hoteles, centros de reuniones o cualquier otro lugar público.

Tipo de Activo	Ejemplos
locaciones que contienen a los activos y procesos, así como los medios físicos necesarios para operar	**Ambiente Interno.** Se refiere al lugar delimitado por el perímetro de la organización del ambiente externo. Puede ser un área protegida creada a través de barreras físicas o medios de vigilancia. Por ejemplo, establecimientos y edificios.
	Zonas. Se refiere al espacio delimitado por barreras físicas formando divisiones dentro del ambiente interno de la organización. Se obtienen creando barreras físicas dentro de las estructuras de tratamiento de los datos personales. Por ejemplo: oficinas, zonas de acceso restringido, zonas seguras.
	Servicios esenciales y utilidades. Servicios y medios requeridos tanto para proveer de energía a los equipos de sistemas de información y sus periféricos como aquéllos requeridos para la subsistencia de operaciones y personal. Por ejemplo, suministro de agua, electricidad, aire acondicionado, manejo de desechos.
Personal y Organización **Consiste en todas las personas involucradas en la operación del Sistema de Gestión de Datos Personales, así como sus funciones, roles o procedimientos asignados**	**Custodios.** Son aquéllos con responsabilidad funcional sobre los activos de información y de apoyo. Por ejemplo: la persona encargada de procesar la nómina de los empleados o bien o el administrador de base de datos del negocio encargado de generar los reportes mensuales de clientes prospectos.
	Usuarios. Personas que utilizan los activos en el contexto de su actividad y quienes tienen responsabilidad específica al respecto. Pueden tener privilegios especiales sobre los sistemas de información para cumplir con sus tareas cotidianas. Por ejemplo: recursos humanos, áreas financieras, gerentes.
	Personal Técnico. Personas a cargo de la operación, mantenimiento y desarrollo de los sistemas de información. Tienen privilegios de acceso o implementación especial para poder cumplir con sus tareas cotidianas. Por ejemplo: administrador de sistemas, administrador de datos, respaldo, mesa de soporte técnico, oficiales de seguridad, programadores.
	Estructura de la organización. Está constituida por las diferentes ramas de la organización, incluyendo actividades multifuncionales de la administración. Ejemplos: Recursos humanos, departamento de TI, compras, unidad de negocios, seguridad de instalaciones, cuerpos de auditoría.
	Proyectos o sistemas de la organización. Consiste en los grupos que surgen para determinados proyectos o servicios. Ejemplos: Proyecto para una nueva aplicación de negocio, proyecto de protección civil, equipo para la migración de sistemas.
	Contratistas/ proveedores/ terceros. Son organizaciones ajenas que proveen con servicios o recursos a través de un contrato. Ejemplos: administración, almacenamiento de datos, consultores, servicios de soporte técnico de tecnología no propietaria.

Anexo B. Ejemplos de Amenazas Típicas

Se debe prestar particular atención a las amenazas de origen humano, las cuales están especialmente representadas en la siguiente tabla:

Origen de la Amenaza	Motivación/Causa	Posibles Consecuencias
Hacker, cracker	• Desafío • Dinero • Ego • Estatus • Rebelión	• Acceso no autorizado al sistema • Ingeniería social • Intrusión en los sistemas • Robo de información
Criminal computacional	• Alteración no autorizada de información • Destrucción de información • Ganancia económica • Revelación ilegal de información	• Acciones fraudulentas, robo • Extorción y chantaje, acoso • Intrusión a los sistemas informáticos • Sobornos de información • Suplantación de identidad • Venta de información personal
Terrorista	• Chantaje • Destrucción • Explotación • Ganancia política • Reconocimiento mediático • Venganza	• Ataque a personas y/o instalaciones (por ejemplo, bomba) • Ataque a sistemas (por ejemplo, denegación de servicio) • Manipulación de los sistemas • Penetración a los sistemas
Espía industrial (inteligencia empresarial, gobiernos extranjeros, robo de tecnología, etc.)	• Espionaje económico • Ventaja competitiva	• Acceso no autorizado a información clasificada o propietaria • Explotación económica • Ingeniería social • Intrusión a la privacidad del personal • Penetración a los sistemas

Origen de la Amenaza	Motivación/Causa	Posibles Consecuencias
		• Robo de información • Ventaja política
Interno (Personal con poco entrenamiento, descontento, negligente, deshonesto o empleados despedidos)	• Curiosidad • Ego • Errores no intencionales u omisiones (por ejemplo, errores de captura de información, errores de programación) • Ganancia económica • Venganza	• Abuso en la operación de los sistemas • Acceso no autorizado a los sistemas • Ataque a empleados y/o instalaciones • Chantaje • Código malicioso • Consulta de información clasificada o propietaria • Datos incorrectos o corruptos • Errores en los sistemas • Fraude y robo • Intercepción de comunicaciones • Intrusiones a sistemas • Sabotaje de los sistemas • Sobornos de información • Venta de información personal

En la siguiente tabla se presentan algunos ejemplos de amenazas típicas, los cuales pueden ser usados durante el proceso de identificación y evaluación de amenazas.

Es importante aclarar que distintas amenazas podrían interrelacionarse en función de un activo, y que no existe ningún orden prioritario entre los tipos y grupos de amenazas. Por ejemplo, un activo podría ser afectado por una amenaza de sismo (Eventos Naturales), al mismo tiempo que por una amenaza de fuego (Daño Físico), y a su vez afectarse por la pérdida de suministro eléctrico (Pérdida de Servicios Básicos).

Tipo	Amenazas
Daño Físico	Fuego
	Agua
	Contaminación
	Accidentes
	Polvo, corrosión, humedad, congelamiento
Eventos Naturales	Fenómenos climáticos o meteorológicos
	Fenómenos sísmicos
	Fenómenos volcánicos
Pérdida de Servicios Básicos	Falla en el sistema de aire acondicionado o suministro de agua
	Pérdida de suministro eléctrico
	Falla en los equipos de telecomunicaciones
Información comprometida por fallas técnicas	Intercepción e interferencia de señales
	Espionaje remoto
	Escucha en comunicaciones
	Robo de medios o documentos
	Robo de equipo
	Recuperación de medios desechados o reciclados
	Revelación
	Fuentes poco confiables para la obtención de datos
	Alteración de hardware
	Alteración de software
	Rastreo de localización
	Fallas del equipo
	Malfuncionamiento del equipo
	Saturación de los sistemas de información
	Malfuncionamiento del software
	Falla en el mantenimiento del sistema de información
Acciones no Autorizadas	Uso no autorizado de equipo
	Uso de software copiado o falsificado

Tipo	Amenazas
	Corrupción de datos
	Procesamiento ilegal de los datos
Compromiso de las Funciones	Error de uso
	Abuso de privilegios
	Falsificación de privilegios
	Denegación de acciones

Anexo C. Ejemplos de Escenarios

La siguiente tabla presenta escenarios de incidente, donde se muestran ejemplos de amenazas que podrían explotar una vulnerabilidad.

Es importante enfatizar que según el contexto de la organización, podrían existir otras amenazas que exploten las vulnerabilidades mencionadas, también pueden existir otras amenazas y vulnerabilidades específicas para cada organización. Asimismo, para poder ponderar el riesgo, las organizaciones deben evaluar el potencial o probabilidad de que cierto escenario de incidente ocurra.

Ejemplo para la lectura de la tabla:

Un **Activo** de apoyo de **tipo Hardware** (computadora) es **Vulnerable** debido a *Mantenimiento insuficiente* del equipo y, por ello, existe una **Amenaza** de *Falla en el sistema de información personal*, lo cual puede ocasionar la **pérdida o daño** de los datos personales.

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
Hardware	Mantenimiento insuficiente	Falla en el sistema de información personal	Pérdida o daño
	Falta de un procedimiento para la sustitución de equipos	Falla de los equipos	Pérdida o daño
	Susceptibilidad a daño físico	Polvo, corrosión, congelamiento, fuego, agua, contaminación, radiación electromagnética.	Pérdida, destrucción o daño
	Falta de configuraciones adecuadas al equipo	Falla en el funcionamiento del equipo	Pérdida, destrucción, acceso o uso no autorizado
	Susceptibilidad a los cambios de voltaje	Pérdida de suministro eléctrico	Pérdida o destrucción
	Susceptibilidad a las variaciones del ambiente	Fenómenos meteorológicos	Pérdida, destrucción o daño
	Almacenamiento no cifrado	Robo de soportes electrónicos	Robo, extravío o copia no autorizada / Uso, acceso o tratamiento no autorizado
	Falta de cuidado en la destrucción de soportes electrónicos	Robo de información y/o soportes electrónicos	Robo, extravío o copia no autorizada / Uso, acceso o tratamiento no autorizado

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
Software	Carencia o falta de pruebas al software y su configuración antes de su liberación	Error en el funcionamiento de la aplicación	Daño, alteración o modificación
	Falta de actualizaciones de seguridad en software	Abuso de privilegios por parte de los usuarios	Uso, acceso o tratamiento no autorizado
	No cerrar la sesión al abandonar la estación de trabajo	Acceso no autorizado a los sistemas	Uso, acceso o tratamiento no autorizado
	Desecho o reutilización de medios de almacenamiento sin un adecuado borrado de información	Consulta de información confidencial	Robo, copia, uso, acceso o tratamiento no autorizado
	Falta de registros de auditoría	Acciones fraudulentas	Uso, acceso o tratamiento no autorizado
	Error en las asignaciones de privilegios de acceso	Intrusión en los sistemas	Uso, acceso o tratamiento no autorizado
	Interfaces de usuario complicadas	Error en la operación de los sistemas	Uso, acceso o tratamiento no autorizado, daño, alteración o modificación
Redes	Falta de mecanismos de identificación y autenticación de usuario	Suplantación de identidad	Pérdida, destrucción robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado daño, alteración o modificación
	Contraseñas no cifradas	Penetración y manipulación de los sistemas	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Servicios de red innecesarios habilitados y/o mal uso de protocolos	Intrusión a la privacidad del personal	Uso, acceso o tratamiento no autorizado

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
	Falta de monitorización de los componentes de las redes, protocolos, servicios y aplicaciones	Canales encubiertos y tráfico clandestino	Uso, acceso, o tratamiento no autorizado
	Descarga y uso de software no controlado	Ejecución de código malicioso	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de respaldos	Corrupción de datos en los sistemas	Pérdida o destrucción Daño, alteración o modificación
	Falta de un registro sobre la administración de los recursos	Uso no autorizado de los servicios	Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado
	Líneas de comunicación sin protección	Espionaje o escucha de comunicaciones	Uso, acceso o tratamiento no autorizado
	Cableado de interconexión dañado o antiguo	Malfuncionamiento en los equipos de telecomunicaciones	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Arquitectura de red insegura	Espionaje o escucha de comunicaciones	Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado
Personal	Falta de personal sensibilizado y/o entrenado en Seguridad	Fraude y robo	Uso, acceso o tratamiento no autorizado
	Proceso de reclutamiento inadecuado	Fraude y robo	Pérdida o destrucción Robo, extravío o copia no autorizada

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
			Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Uso incorrecto de software y hardware	Error en las operaciones de los sistemas	Pérdida o destrucción Daño, alteración o modificación
	Falta de supervisión al trabajo de externos	Robo de información y/o soportes físicos/electrónicos	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de políticas acerca del uso de medios de telecomunicaciones	Uso no autorizado de equipo	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
Sitio	Falta o implementación inadecuada de controles de acceso	Robo o destrucción de activos	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Lugar susceptible al daño por agua	Inundaciones	Pérdida o destrucción
	Red eléctrica inestable	Variación de voltaje	Pérdida o destrucción
Organización	Falta de procedimientos formales para la administración de privilegios de usuario	Abuso de privilegios por parte de los usuarios	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
	Falta o insuficiencia de previsiones en la realización de contratos con clientes y/o terceros	Abuso de privilegios por parte de clientes y/o terceros	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de procedimientos formales de monitoreo y/o auditoría	Riesgos no identificados	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta o ausencia de reportes de fallas	Reincidencia de problemas	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de procedimiento formal para documentar y supervisar un SGSDP	Malfuncionamiento del SGSDP	Pérdida o destrucción Daño, alteración o modificación
	Falta de asignación de responsabilidades respecto a la seguridad de la información	Abuso de privilegios por parte de los usuarios	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de políticas de uso de correo electrónico	Fuga de información	Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado
	Falta de procedimientos para la instalación y actualización de los	Fallas en los sistemas de información	Pérdida o destrucción Robo, extravío o copia no

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
	sistema de información		autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de registros de actividad/bitácoras en los sistemas de administración u operación	Abuso de privilegios por parte de los usuarios	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de procesos para el tratamiento de datos personales	Incumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta o insuficiencias de condiciones relacionadas a la protección de datos en contratos con empleados	Empleado negligente	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de procesos estrictos en caso de un incidente o vulneración de seguridad	Malfuncionamiento del SGSDP	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de políticas para el uso de activos fuera de la organización	Robo de datos personales	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas	Posible vulneración a los datos personales
			autorizado Daño, alteración o modificación
	Falta de mecanismos de monitoreo para vulneraciones a la seguridad de los datos	Intrusión de personas malintencionadas	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación
	Falta de procedimientos para reportar puntos débiles en la seguridad	Código malicioso	Pérdida o destrucción Robo, extravío o copia no autorizada Uso, acceso o tratamiento no autorizado Daño, alteración o modificación

Anexo D. Ejemplos de Controles de Seguridad

Las medidas de seguridad identificadas en el paso 6, según lo establecido en el inciso III del artículo 61 del Reglamento, podrán estar basadas en los controles presentados en el presente anexo. La organización deberá elegir los controles administrativos, técnicos o físicos que le permitan atender de mejor manera los riesgos identificados y minimizar las consecuencias de posibles vulneraciones.

La siguiente tabla de controles de seguridad es opcional y se puede usar como referencia en la elaboración del plan de tratamiento del riesgo, en la valoración del riesgo, o incluso para establecer el contexto de seguridad de la organización en función de la presencia o ausencia de los controles siguientes. Sin embargo, las organizaciones deberán asegurarse de que no pasaron por alto la implementación de medidas que permitan atender riesgos que posiblemente no identificaron durante el análisis de riesgos.

Objetivo de Control	Descripción
Políticas del SGSDP	
Políticas de gestión de datos personales	Deben existir políticas aprobadas por la Alta Dirección para la regulación específica, condiciones contractuales, así como para la creación, implementación y mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales y sus activos relacionados durante el tratamiento, que sirvan como guía organizacional del propósito, objetivos, responsabilidades y compromisos establecidos por los involucrados para el cumplimiento de la normatividad aplicable a los datos personales.
Revisión y evaluación	Las políticas relacionadas con el SGSDP deben ser revisadas y evaluadas en su efectividad y cumplimiento periódicamente, así como cuando surja un nuevo riesgo o cambio significativo en la organización.
Documentación del SGSDP	Se deben identificar y documentar de manera proporcional a la organización los activos, políticas, acuerdos, planes estratégicos, procedimientos, controles de seguridad, y todo proceso relacionado al SGSDP.
Cumplimiento legal	
Identificación de legislación/regulación aplicable	Se deben identificar y documentar los deberes y responsabilidades de toda la organización para cumplir con los requerimientos legales y contractuales relacionados con la protección de datos personales. Se debe poner especial atención en la legislación relacionada con la propiedad intelectual, industrial, privacidad y protección de datos personales a nivel nacional e internacional. También se debe considerar la regulación específica de un sector o rama industrial, por ejemplo, legislación aplicable a datos de salud.
Salvaguarda de registros organizacionales	Se debe mantener el resguardo de todos los registros y documentación que pudieran ser evidencia o bien, requeridos en cumplimiento de la LFPDPPP y protegerlos contra pérdida, destrucción, falsificación, acceso o revelación no autorizados.

Objetivo de Control	Descripción
Prevención del mal uso de activos	Se deben tener mecanismos contra el uso de activos para propósitos no autorizados, por ejemplo, para sistemas electrónicos, utilizar bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permisos e informar mediante un mensaje el uso indebido.
Recolección de evidencia	Se deben tener procesos para la recolección de evidencia según las mejores prácticas en caso de una vulneración o incidente de seguridad.
Revisión de cumplimiento técnico	Se deben revisar los activos y sus controles de seguridad, tal que se verifique su correcto funcionamiento así como las posibles amenazas y vulnerabilidades relacionadas.
Controles de auditoría de sistemas	Se debe tener un proceso para la revisión y evaluación del funcionamiento del SGSDP, tal que se minimicen las consecuencias de posibles vulneraciones y se logre un ciclo de mejora continua.
Protección del soporte de auditoría del sistema	Se deben proteger las herramientas, el software y los archivos de datos que surjan o se utilicen en una auditoría, para evitar comprometer la seguridad de la información de la organización.
Estructura organizacional de la seguridad	
Administración y Coordinación de la seguridad de la información	La Alta Dirección debe tener claros sus objetivos y soportar las iniciativas generadas por su equipo, apoyados en la comunicación efectiva entre las diferentes áreas de la organización para la implementación de controles de seguridad, coordinados por la persona a cargo de la seguridad de la información personal.
Designación de deberes en seguridad y protección de datos personales	Se deben designar deberes y obligaciones respecto a los individuos que intervengan en el uso y protección de datos personales.
Recomendaciones de un especialista en seguridad de la información	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.
Cooperación con organizaciones	En su caso, buscar la colaboración de autoridades, cuerpos regulatorios, servicios de información o de telecomunicaciones, entre otros para definir las acciones apropiadas en caso de un incidente o vulneración de seguridad.
Revisión de implementación	Realizar una revisión periódica de la implementación del SGSDP por auditores internos o externos.
Identificación de riesgos de terceros	Identificar el alcance de involucramiento que pueden tener terceros en el tratamiento de los datos personales y analizar si es justificado y bajo el consentimiento del titular.

Objetivo de Control	Descripción
Requerimientos de seguridad en contratos con terceros	Cuando se establezca un contrato con un tercero, revisar las clausulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la organización. Se debe revisar el contrato generado entre la organización y el prestador respecto al nivel de servicio, incluyendo cualquier actualización de los términos y condiciones. Esto es importante en el caso de la designación de encargados por parte de un responsable de datos personales.
Requerimientos de seguridad en contratos con servicios de almacenamiento de información y computo en la nube	Cuando se establezca un contrato con un prestador de servicios de almacenamiento de información y/o de computo en la nube, además de revisar las clausulas referentes a los requerimientos de seguridad y de tratamiento de datos personales, de manera particular hay que: verificar el nivel de acceso que tiene el prestador y limitar el tratamiento a lo estrictamente necesario para el cumplimiento de las condiciones del servicio; verificar el ciclo de vida de la información (por ejemplo, donde se almacena, como se replica, como se elimina en un ambiente distribuido, como se garantiza la eliminación de la información) y la ubicación física de la infraestructura del prestador.
Clasificación y acceso a los activos	
Inventario y clasificación de datos personales	Mantener un registro de los datos personales recolectados y tratados por la organización en cualquier soporte físico o electrónico, teniendo especial atención en los datos sensibles, financieros y patrimoniales.
Inventario de activos	Mantener un registro de los activos de información y de soporte. Identificar a los individuos o grupos de personas dentro o fuera de la organización con responsabilidad sobre los activos.
Identificación de procesos de datos personales	Se debe tener identificado el ciclo de vida de los datos personales en cada uno de sus procesos, desde la obtención, almacenamiento, procesamiento, cancelación o cualquiera que sea su tratamiento. Esto es especialmente importante para conocer dónde se resguardan y qué se hace con los datos personales, lo cual contribuye también en agilizar la respuesta al ejercicio de los derechos ARCO por parte de un titular.
Seguridad del personal	
Identificar responsabilidades de seguridad en cada puesto de trabajo	Establecer y dar a conocer a cada, función, rol o puesto las responsabilidades que corresponden respecto a la seguridad y protección de datos personales, informando en su caso de las sanciones de incumplimiento de la política de seguridad.
Revisión de contratación del personal	Revisar el perfil del personal que será contratado por la organización, esto debe incluir referencias (personales y/o laborales), la confirmación de títulos académicos y profesionales así como los controles de identidad y antecedentes.
Acuerdo de confidencialidad	Se debe firmar un acuerdo de confidencialidad o no revelación de información por los nuevos empleados de la organización involucrados en el tratamiento de los datos personales.

Objetivo de Control	Descripción
Términos y condiciones de empleo	Dentro de los términos de contratación, la organización debe informar ampliamente a los nuevos empleados sobre sus deberes y compromisos respecto a la seguridad de la información y protección de datos personales. También deberá considerarse la presentación de un aviso de privacidad al personal interno del cual recabaremos datos personales de distintos tipos.
Entrenamiento y educación	Empleados, contrataciones externas y usuarios en general deben recibir concienciación y entrenamiento apropiado respecto a la seguridad de la información y protección de datos personales.
Proceso disciplinario	Debe existir un proceso disciplinario en la organización para aquellos que no cumplan o violenten lo establecido en la política o procedimientos.
Seguridad física y ambiental	
Perímetro de seguridad	Identificar o en su caso, implementar mecanismos de seguridad en el perímetro de la organización, por ejemplo bardas, puertas con control de acceso, vigilancia por guardias de seguridad, etc.
Control de entrada física	Implementar mecanismos que sólo permitan el acceso a personal autorizado, por ejemplo a través de dispositivos biométricos, tarjetas inteligentes, personal de seguridad, etc.
Seguridad en entornos de trabajo	Implementar mecanismos para mantener las áreas de resguardo o servicios de procesamiento de datos, aisladas de amenazas causadas por el hombre. Por ejemplo, puertas con cerradura, gabinetes o cajas de seguridad. Además deben existir mecanismos para proteger a los activos de fenómenos como el agua, fuego, químicos, vibraciones, radiación, etc. Por ejemplo, extintores, detectores de humo, etc. Así como cierto monitoreo ambiental y de medidas comunes, como no introducir alimentos y bebidas en áreas restringidas.
Trabajo en áreas restringidas	Los activos de información sólo deben ser accesibles por personal que los requiera en sus deberes en la organización o bien por un tercero autorizado. Por lo tanto, debe existir acceso controlado para personal trabajando en un área restringida.
Seguridad del cableado	Verificar el buen estado de las conexiones de telecomunicaciones o de transmisión de información, para evitar intercepción o falla en el servicio.
Mantenimiento del equipo	Asegurarse de que los activos secundarios reciban mantenimiento periódicamente, (por ejemplo, según indicaciones del fabricante), además de realizarse por personal autorizado.
Aseguramiento de los activos fuera de las instalaciones	Se deben establecer mecanismos autorizados por la Alta Dirección, para controlar la salida fuera de las instalaciones de cualquier activo que contenga datos personales, considerando que su seguridad sea equivalente al menos a la establecida dentro de la organización.
Borrado seguro de información	Cuando se elimine un activo como equipo de procesamiento, soporte físico o electrónico, deben aplicarse mecanismos de borrado seguro, o bien, de destrucción adecuado. Cualquier eliminación de activos debe registrarse con fines de auditoría.

Objetivo de Control	Descripción
Escritorio limpio	Cualquier documento o activo de información crítico debe estar resguardado, fuera de la vista, cuando éste no sea atendido.
Robo de propiedad	Revisar e identificar los activos, como equipo o software que sean susceptibles de sustracción de las instalaciones.
Gestión de comunicaciones y operaciones	
Control de cambios operacionales	Debe existir un procedimiento para discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales.
Segregación de tareas	En relación a la estructura de la organización se deben segregar y aislar los puestos y responsabilidades del personal que realice tratamiento de datos personales, con el fin de reducir las oportunidades de un uso indebido de los activos.
Separación del área de desarrollo de sistemas de datos personales	Las instalaciones de desarrollo y /o pruebas deben estar aisladas de las áreas operacionales. Por ejemplo, el software de desarrollo debe estar en una computadora diferente al software de producción. La separación puede hacerse a varios niveles, como utilizar distintos segmentos de red, dividir las instalaciones físicas o por separación de activos.
Administración externa de instalaciones	Se deben identificar los riesgos derivados del servicio de administración de instalaciones prestado por un proveedor (por ejemplo, instalaciones eléctricas o telefonía). En caso de que se identifique algún riesgo, debe ser discutido con el externo para incorporar los controles adecuados.
Estándares de configuración segura y actualización de sistemas.	Se deben tener identificadas las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Es recomendable realizar pruebas antes de implementar cualquiera de ellos. También deberán verificarse que los sistemas que soportan el tratamiento de datos personales cuentan con configuraciones seguras en el hardware, sistema operativo, base de datos y aplicaciones.
Protección contra software malicioso	Deben existir diferentes controles respecto al software malicioso: Prohibir el uso de software ilegal y/o no autorizado. Aplicar difusión (campañas, boletines) sencillos para advertir del software malicioso. Mantener en los dispositivos de procesamiento de información como computadoras, las respectivas herramientas actualizadas que las protejan contra software malicioso. En su caso, monitorear el tráfico y las actividades de red para descubrir cualquier comportamiento anómalo, tales como virus, descargas de contenido inapropiado, fugas de información, etc.

Objetivo de Control	Descripción
Respaldo de la información	Deben establecerse respaldos proporcionales al modelo de negocio y manejo de datos personales. Se debe tener un adecuado control sobre la periodicidad de generación de respaldos y el respectivo almacenaje de los soportes físicos/electrónicos, especialmente para el ejercicio de derechos ARCO. Se debe tener identificado el proceso a realizar en caso de que sea necesario restaurar un respaldo, asimismo, se deben probar los respaldos periódicamente para asegurar su correcto funcionamiento.
Registros de operadores	Los administradores de los sistemas de datos personales deben poder acceder a los registros de las actividades dentro del mismo, para analizarlos periódicamente.
Registro de fallas	Las fallas en sistemas y activos deben poder reportarse y gestionarse, esto incluye la corrección de la falla y revisión de los registros.
Controles de red	Cuando aplique, debe existir separación entre los segmentos de red y administración de recursos de red. Deben existir procedimientos y responsabilidades para el manejo de conexiones remotas. Se debe buscar la implementación de controles especiales para salvaguardar la confidencialidad e integridad de las comunicaciones sobre redes públicas (por ejemplo, redes privadas virtuales, métodos de cifrado, etc.)
Gestión de soportes informáticos extraíbles	Deben existir políticas y procedimientos para el uso de soportes informáticos extraíbles como memorias USB, discos, cintas magnéticas, etc.
Documentación de seguridad del sistema	Toda la documentación de los sistemas y activos de información debe ser protegida de acceso no autorizado.
Seguridad de medios en tránsito	Se debe asegurar el traslado de soportes físicos/electrónicos que contengan datos personales contra robo, acceso, uso indebido o corrupción.
Comercio electrónico seguro	Se deben contar con mecanismos contra la actividad fraudulenta, disputas contractuales o revelación/modificación de información. En los entornos web deben existir mecanismos de autorización y autenticación para las transacciones. Asimismo, debe revisarse las cláusulas de intercambio de datos personales y seguridad en los acuerdos establecidos entre las partes involucradas.
Mensajería electrónica	Se debe hacer uso adecuado del correo electrónico, mensajería instantánea y redes sociales, utilizando mecanismos que permitan bloquear la recepción de archivos potencialmente inseguros, mensajes no solicitados, no deseados o de remitente no conocido.
Seguridad en sistemas electrónicos	Se debe hacer uso adecuado de los sistemas de datos personales a través de guías de uso y gestión de riesgos asociados con dichos sistemas.

Objetivo de Control	Descripción
Divulgación de información de manera pública	Debe existir un proceso de autorización formal para hacer pública información, por cualquier medio de difusión. Cuando se publica un discurso o una nota de prensa, o bien para sistemas de acceso público (por ejemplo, páginas web para publicación de concursos, rifas, entre otros), deben existir mecanismos para que la información mantenga su integridad y que no permita ser el medio para dañar otros activos ubicados dentro de la organización.
Otras formas de intercambio de información	Se debe contar con procedimientos relacionados al intercambio de datos personales, dentro y fuera de la organización a través de diversos medios, como voz, datos, video, etc. El personal debe mantener la confidencialidad de información sensible y datos personales en cualquier intercambio de información.
Disociación y Separación	Se deben aislar los datos de manera que por sí mismos no aporten información valiosa de un titular o éste no pueda ser identificable. También pueden ser separados los activos de información grandes en activos de información más pequeños (por ejemplo, una base de datos de clientes en dos bases de datos, clientes corporativos y personas físicas). Entre mayor cantidad de información tiene un activo, éste resulta más atractivo para un atacante.
Control de acceso	
Reglas de control de acceso	Deben existir reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades.
Gestión de usuarios y contraseñas	Cada usuario debe tener un identificador único en el sistema al cuál se vincularán sus privilegios y acceso. Asimismo, cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso (cuando aplique, los usuarios tendrán que firmar acuerdos que los obliguen a mantener sus contraseñas en secreto). Los usuarios deben tener guías o recomendaciones para la creación y mantenimiento de contraseñas seguras. Se deben tener procedimientos para la administración de usuarios (altas, bajas y modificaciones) en los sistemas de información, en su caso, además deben existir controles respecto a las contraseñas entregadas al personal, clientes, proveedores, prestadores de servicios o cualquier usuario del sistema de datos personales, (por ejemplo rendición de cuentas, fortalecimiento de contraseñas, almacenamiento cifrado de contraseñas, etc.)
Gestión de privilegios	En un ambiente multiusuario se deben conceder privilegios en función de los roles y responsabilidades de cada usuario o grupo de usuarios para el cumplimiento de sus deberes, sin que se exponga a acceso, eliminación copia o alteración no autorizados a otros activos de información.
Revisión de privilegios de usuarios	Debe existir un proceso de revisión para verificar el adecuado y no excesivo uso de los privilegios de cada usuario en función de sus roles y responsabilidades, por ejemplo una persona con privilegios especiales puede ser revisada cada 3 meses, mientras que un usuario estándar cada 6 meses.

Objetivo de Control	Descripción
Equipos sin atender	Los usuarios y contrataciones externas deben tener conocimiento de las medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, por ejemplo cerrar la sesión cuando se ha terminado de trabajar en la computadora, bloquear el equipo automáticamente cuando no se usa por largos periodos de tiempo, etc.
Uso de servicios de red	Deben existir reglas respecto al acceso autorizado a las redes y servicios disponibles así como los procedimientos de uso y conexión.
Ruta reforzada	Cuando aplique, deben existir mecanismos para asegurar un camino único de interconexión entre dispositivos.
Autenticación de usuario para conexiones externas	Deben existir mecanismos para asegurar las conexiones que se hagan a través de redes externas a la organización, por ejemplo, cifrado, protocolos de autenticación por desafío mutuo, etc.
Autenticación de nodo	Si es el caso, aplicar un método de autenticación alternativo para grupos de usuarios remotos que se conecten a una instalación segura u ordenador compartido.
Segregación de redes	La red debe segregar a los usuarios a través de mecanismos como VPN o firewalls, por ejemplo, la red externa para usuarios de visita debe encontrarse en un segmento de red distinto de la red donde se encuentran los sistemas de datos personales.
Protocolos de conexión de red	Se deben vigilar los protocolos de conexión de redes compartidas que se expanden más allá de la organización, por ejemplo para el correo electrónico o para el acceso a internet.
Protocolos de enrutamiento	Se debe vigilar la existencia de mecanismos para asegurar que las conexiones de computadoras y flujos de información no vulneren el control de acceso a la organización.
Seguridad de servicios de red	La organización debe obtener una clara estructura y descripción de los servicios de red públicos o privados, sus características y atributos de seguridad.
Identificación automática de terminales	Contar con un mecanismo de red interna para autenticar cualquier tipo de conexión.
Proceso de inicio de sesión	Sólo se debe tener acceso a los sistemas de datos personales a través de un inicio de sesión seguro, esto minimiza los accesos no autorizados.
Alerta de coerción a usuarios	Cuando aplique, considerar alertas para usuarios cuyos privilegios los hagan objetivo de coerción.
Tiempo límite de terminal	Aquellas terminales que estén expuestas en áreas de acceso general deben configurarse para limpiar la pantalla o bloquearse después de un periodo de inactividad.
Tiempo límite de conexión	Debe existir un tiempo límite de acceso al sistema de datos personales, especialmente para conexiones desde terminales o dispositivos fuera del perímetro de la organización.

Objetivo de Control	Descripción
Restricción de acceso a datos personales	El acceso a datos personales a través del personal o aplicaciones debe ser definido en consistencia con la política de seguridad de los datos personales, limitando el uso de información a las responsabilidades específicas.
Trazabilidad de tratamiento	La trazabilidad y posibilidad de identificar quién tuvo acceso a los datos personales y los tratamientos realizados.
Aislamiento de sistemas sensibles	Se deben evaluar los sistemas y activos que por su naturaleza deban desarrollarse en ambientes aislados, por ejemplo equipos ejecutando aplicaciones críticas, datos personales sensibles, o información confidencial fuera de entornos de red.
Registro de eventos	Se deben generar registros de excepciones y eventos relevantes de seguridad en los sistemas y activos, los cuales deben almacenarse un periodo acordado para investigación y control de acceso.
Monitorear el uso del sistema	Debe haber procedimientos para el monitoreo del uso correcto de los activos y el adecuado comportamiento de los sistemas. Los usuarios sólo deben hacer las actividades para las cuales están explícitamente autorizados.
Sincronización de relojes	Cuando los sistemas de cómputo o telecomunicaciones operen con relojes en tiempo real se debe acordar un estándar de tiempo y horario. Esto ayuda a la revisión de registros y auditoría.
Dispositivos móviles internos.	Se debe considerar el trabajo externo a través de dispositivos móviles (por ejemplo netbooks, laptops, tablets, smartphones) proporcionados a los usuarios por la organización. Esto incluye capacitación sobre la responsabilidad y medidas de seguridad relacionadas a su uso y las consecuencias de su pérdida. Asimismo limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la organización, previamente autorizadas por la Alta Dirección.
Dispositivos móviles externos.	Deben existir mecanismos para la incorporación de dispositivos personales ingresados por los usuarios al entorno de la organización, así como para el tratamiento de datos a través de dichos dispositivos. Se debe limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la organización, previamente autorizadas por la Alta Dirección. En su caso, los dispositivos que interactúen con los activos de la organización deberán reforzarse, si un dispositivo no puede acoplarse a los sistemas de información o genera una vulneración, deberá excluirse.
Almacenamiento privado dentro del entorno de operación	Se deben establecer reglas para limitar el uso de servicios privados de los usuarios (por ejemplo, el uso de la cuenta de correo electrónico gratuita) para evitar el almacenamiento o transferencia no autorizados de datos personales. Se debe procurar exclusivamente el uso de servicios dentro de entornos empresariales o en los cuales exista un contrato con el prestador del servicio, siempre dentro de las condiciones de las políticas de seguridad de datos personales establecidas en la organización.
Teletrabajo	En su caso, se deben especificar las condiciones de seguridad y procesos relacionados al teletrabajo, como el robo de equipos, las conexiones seguras, cláusulas de confidencialidad, etc.

Objetivo de Control	Descripción
Desarrollo y mantenimiento de sistemas	
Validación de datos de entrada	Cuando se proporcionen datos a un sistema, se debe validar que estos sean ingresados de forma correcta, tal que no produzcan conflictos de tratamiento posteriores. En el caso de aplicaciones, se debe asegurar que los métodos de entrada sean seguros y no produzcan vulnerabilidades.
Autenticación de mensajes	En los sistemas de información deben existir mecanismos de autenticación de mensajes para asegurar que un mensaje proviene de una fuente autorizada o que no está corrompido.
Validación de datos de salida	En el caso de aplicaciones se debe asegurar que los datos entregados sean los esperados y que se proporcionen en las circunstancias adecuadas.
Cifrado	Deben existir reglas que definan el uso de cifrado en comunicaciones y/o almacenamiento, así como de los controles y tipos de cifrado a implementar. Se debe identificar la sensibilidad de los datos y el nivel de protección necesario para aplicar el cifrado correspondiente, en almacenamiento y/o transferencia de información.
Firmas electrónicas	Se pueden utilizar firmas electrónicas o digitales para ayudar a la autenticidad e integridad de documentos electrónicos.
Servicios de no-repudio	Es un servicio de seguridad que permite probar la participación de las partes involucradas en una comunicación. Se deben gestionar las disputas que puedan surgir de negar o afirmar la participación de alguien en un evento o acción.
Control de software y sistemas	Se deben tener controles y procesos para integrar software al ambiente operacional, para minimizar el riesgo de corrupción de datos. Se debe probar cualquier cambio o actualización de sistemas críticos antes de implementarse en la organización. Se deben aplicar los cambios a una copia concreta del software original y evaluar su funcionamiento.
Protección de datos de prueba del sistema	Se debe vigilar y gestionar los datos que se utilicen para fines de prueba, evitando el uso de bases de datos con datos personales para tales propósitos, si es necesario usar datos personales, se deben desvincular de su titular antes de usarse.
Control de acceso a software de configuración	Se debe restringir el acceso a los usuarios no especializados a las carpetas que mantienen la configuración de las aplicaciones o sistemas como las librerías, con el fin de prevenir corrupción en los archivos o software.
Canales encubiertos y código malicioso	Se deben tener mecanismos para asegurar que con nuevas actualizaciones no se introduzcan canales de comunicación para virus y código malicioso.
Contratación de servicios de software	Se debe tener bien definido y actualizado el arreglo de contratación de servicios de software como pueden ser las licencias de uso, pruebas antes de instalación, requerimientos del sistema, detección de virus y código malicioso, etc.

Objetivo de Control	Descripción
Vulneraciones de seguridad	
Procedimientos para el manejo de incidentes	Deben existir procedimientos para el manejo de incidentes, tal que la respuesta sea pronta y efectiva, llevando a cabo un registro para diferenciarlos, de manera que posteriormente se puedan conducir revisiones y comparaciones.
Procedimientos de acción en caso de incidente	Deben existir procedimientos relacionados al monitoreo, reporte, mitigación y documentación de un incidente de seguridad, tal que se pueda verificar la ocurrencia de una vulneración para darle un adecuado seguimiento e implementar las medidas de seguridad correctivas.
Reporte de incidentes de seguridad	Debe existir una manera formal de reportar incidentes de seguridad de acuerdo a la cadena de mando establecida.
Reporte de fallas en funcionamiento	Debe existir una manera formal de reportar fallas en funcionamiento de hardware y/o software de acuerdo a la cadena de mando establecida.
Procedimientos de notificación de vulneraciones de seguridad a titulares	Deben existir procedimientos relacionados a la notificación de vulneraciones a los titulares cuando éstas afecten sus derechos patrimoniales o morales. Estos procedimientos deben contemplar la magnitud de la vulneración y los mecanismos que se deban poner a disposición de los afectados.
Aprendizaje de incidentes	Cuando aplique, establecer mecanismos para monitorear, el tipo, volumen y costo de los incidentes de seguridad.
Procedimientos de actualización de SGSDP	Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar el SGSDP.