GUÍA
PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

SECTOR PÚBLICO

inai

Directorio

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

Secretaria de Protección de Datos Personales

Dirección General de Prevención y Autorregulación

Dirección de Seguridad de Datos Personales del Sector Público

Av. Insurgentes 3211,
Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán,
Ciudad de México, C. P. 04530.

Edición, octubre de 2024

Nota

Este documento se elabora a partir del contenido de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales del Sector Público, en lo que refieren al deber de seguridad y particularmente la implementación de un sistema de gestión, asimismo, considera el contenido de diversos estándares internacionales y metodologías en la materia, así como en la Guía de apoyo para la elaboración del Documento de Seguridad, las Recomendaciones en materia de seguridad de datos personales, la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (Sector Privado, versión de junio de 2015) , y la Guía de Mejores Prácticas en Materia de Protección de Datos Personales con un enfoque práctico.

Índice

1. PRESENTACIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1]; en su artículo 34, establece:

> *"Artículo 34. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales* ***deberán estar documentadas y contenidas en un sistema de gestión.***
>
> *Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia."*

Por otro lado, en los Lineamientos Generales de Protección de Datos Personales para el Sector Público[2], se indica:

> *"Sistema de gestión*
> *Artículo 65. El responsable deberá implementar un sistema de gestión de seguridad de los datos personales a que se refiere el artículo 34 de la Ley General, el cual permita* ***planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad****."*

La normatividad en la materia indica que es deber de los sujetos obligados como responsables del tratamiento, proteger los datos personales a través de la implementación de un Sistema de Gestión. Para ello en la presente guía se orientará a los sujetos obligados a comprender qué es un Sistema de Gestión orientado a la seguridad de la información y por supuesto a los datos personales, y sobre todo a la gestión del riesgo de los activos de información que contienen los datos personales a fin de que puedan poner en marcha un Sistema de Gestión de Seguridad de Datos Personales.

Para ello se debe tener en cuenta que la información que contiene datos personales es información indispensable que está expuesta a múltiples amenazas que son susceptibles de materializarse en riesgos, con diversas consecuencias o afectaciones para las personas titulares de los datos personales.

1 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017 https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

2 Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018 https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Dichas amenazas son parte de nuestra cotidianeidad y más aún de la vida institucional, estas van desde amenazas por desastres naturales, suplantación de identidad, hasta ciberataques como pishing, smishing, ransomware, entre otros, lo cual requiere la implementación de controles o medidas de seguridad físicas, administrativa y técnicas que puedan ser gestionados a través de un adecuado enfoque de seguridad de los datos personales.

Es así como un sistema de gestión para la seguridad de los datos personales involucra la correcta gestión de riesgos de los propios datos personales y de los activos que los soportan.

Para conservar los datos personales y por lo tanto a las personas titulares protegidas es indispensable mantener niveles aceptables de riesgo de la información organizacional que los contiene y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Para ello debe buscarse la preservación de la confidencialidad, integridad y disponibilidad de la información.

En el presente documento, se brinda orientación para la implementación de **un Sistema de Gestión de Seguridad de Datos Personales (SGSDP**), basado en el ciclo de mejora continua, denominado *ciclo Deming* o PHVA (Planear-Hacer-Verificar-Actuar) al cual se hace referencia en múltiples metodologías de estándares internacionales, de las cuales algunas fueron considerados para su elaboración:

- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements[3].
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls [3].
- ISO/IEC 27005:2008, Information Technology–Security techniques– Information security risk management. [3]
- ISO 31000:2018-Gestión del riesgo-Directrices[4]
- ISO GUIDE 73, Risk management – Vocabulary[3]
- ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary[3]
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing[3] Information Technology Systems[5]
- OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security[6].
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT V.3[7] elaborada por el antiguo Consejo Superior de Administración Electrónica de España y actualmente mantenida por la Secretaría General de Administración Digital con colaboración del Centro Criptológico Nacional.

3 ISO- International Organization for Standardization https://www.iso.org

4 ISO/IEC 31000:2018, consulta realizada el 02/04//2024: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

5 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890092

6 https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

7 https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

En ese sentido, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través del presente documento realiza una conjunción de los principios básicos que integran algunos de los estándares señalados con el propósito de ayudar a los responsables y encargados del tratamiento, así como a todo interesado, a comprender los pasos clave para realizar un SGSDP a fin de dar cumplimiento a los deberes contenidos en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (Ley General) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).

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 con la naturaleza y objetivos del sujeto obligado.

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 lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y con apoyo en 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 38, de la misma Ley General, buscando siempre proteger a los titulares.

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 del sujeto obligado, se pueda evaluar el impacto en los datos personales y en los sistemas de tratamiento, así como en los titulares y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Es importante señalar que la implementación de un Sistema de Gestión de Seguridad de Datos Personales es un deber conforme al artículo 34 de la Ley General de Protección de Datos Personales y Posesión de los Sujetos Obligados, no obstante, la estructura propuesta en la presente guía es de carácter voluntario, por lo que los responsables podrán decidir libremente qué metodología o metodologías utilizar para la elaboración del Sistema de Gestión dirigido a datos personales y la gestión de riesgos en su institución a efecto de cumplir con el deber de seguridad de los datos personales, incluso es posible crear una propia. En cualquier caso, dicha metodología debe estar documentada y contener los criterios y factores mínimos que exige la Ley General y los Lineamientos Generales, y podrán referir a los marcos y estándares nacionales e internacionales.

Finalmente, se debe aclarar que el seguimiento de este documento no exime a los sujetos obligados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos y los datos personales que se encuentren bajo su custodia.

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

2.1 Definiciones[8]

Activo: En términos generales, un activo es cualquier elemento que representa un valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones[9].

Para efectos de la presente guía, los activos deben entenderse como los datos personales y sistemas de tratamiento que representan un derecho intrínseco de las personas titulares, y también como los elementos que representan valor para el sujeto obligado, en tanto que con ellos opera la propia entidad.

Bases de datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización[10].

Comité de Transparencia. Instancia a la que hace referencia el artículo 43, de la Ley General de Transparencia y Acceso a la Información Pública[11].

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. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

8 Las definiciones son recuperadas de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público y el Estándar ISO/IEC 27001:2011

9 INCIBE, Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. Fecha de consulta: 02/04/2024. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

10 Definición obtenida del artículo 3, fracción III de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

11 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017 https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Datos personales sensibles. Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Encargado. La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

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.

Ley General o LGPDPPSO. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales. Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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

Organización. Grupo de personas y medios organizados con un fin determinado. Puede referirse al sector privado o sector público; para efectos de la presente guía se debe entender como Organización al sujeto obligado.

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.

Propietario. Personas que tienen a cargo la ejecución de un proceso que involucra el tratamiento de datos personales.

Responsable. Los sujetos obligados a que se refiere el artículo 1 de la Ley General que deciden sobre el tratamiento de 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.

Riesgo inherente: Riesgo intrínseco al activo, sin considerar las medidas de seguridad implementadas.

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 General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Sujeto Obligado. Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley General y los Lineamientos Generales, incluyendo al INAI y los organismos garantes.

Tercero. La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos[12].

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

Tratamiento. Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

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

Unidad de Transparencia. Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

12 Artículo 3, fracción XVI, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación 05 de julio de 2010. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

2.2 Conceptos clave para comprender un Sistema de Gestión de Seguridad de Datos Personales

¿Qué es un sistema de gestión?

Para comprender qué es un sistema de gestión debemos comprender primero qué es la **gestión** y qué es un **sistema.**

Gestión es el conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea y alcanzar objetivos. Un **sistema** por su parte es el conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí, o el conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto[13]. Por lo tanto, un **sistema de gestión (SG)** se define como un conjunto de elementos y actividades interrelacionadas que interactúan para alcanzar los objetivos de una Organización.

Todas las organizaciones, sean públicas o privadas persiguen objetivos sean económicos-empresariales, sociales, ambientales, u otros de acuerdo a su objetivo de creación. En el caso de los sujetos obligados, sus objetivos y atribuciones se encuentran establecidos en la norma como puede ser en la Constitución Política de los Estados Unidos Mexicanos o en las leyes que les rigen. En este último caso, las propias leyes ya indican la gestión a realizar para lograr sus objetivos en las labores estatales, en ese sentido, lo que busca un sistema de gestión es que ese cúmulo de normativa interna y externa que le afecta se ordene de manera consciente a fin de que su operación sea eficaz y eficiente para el cumplimiento de sus atribuciones y objetivos.

Ahora bien, es posible implementar sistemas de gestión en muchas materias como calidad, riesgos ambientales, seguridad de la información, entre otros, en el caso que nos ocupa, en materia de protección o seguridad de los datos personales, para ello, hay que tener claro que los datos personales al ser información, su comprensión debe ser dirigida hacia el concepto de seguridad de la información.

Un sistema de gestión para la seguridad de la información, por ejemplo, se compone de múltiples procesos para implementar, mantener y mejorar de forma continua la seguridad de la información, los sistemas de gestión toman como base los riesgos que afectan a la seguridad de la información en una empresa u organización, en este caso los sujetos obligados, por lo que para implementar uno de datos personales, tendremos que implementar procesos para la seguridad de los datos personales tomando como base igualmente los riesgos que les pueden afectar y que de materializarse, causen un daño a las personas titulares.

En ese sentido, un sistema de gestión de seguridad de datos personales apoya a los sujetos obligados en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades y objetivos

13 Definición obtenida de la RAE, disponible en https://dle.rae.es/sistema

en materia de seguridad de datos personales, ya que está diseñado para mejorar continuamente el desempeño del responsable, mediante la consideración de las necesidades de todas las partes interesadas.

La instauración de un sistema de gestión debe basarse en un modelo de mejora continua, es decir, debe tener carácter cíclico, atenderse continuamente y buscar su mejora en todo momento, es por ello por lo que se propone la implementación del SGSDP en el modelo denominado Ciclo Deming, o "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 y objetivos	Planificar	Se identifican políticas, objetivos, se establecen los criterios de valoración y la metodología para la gestión y tratamiento de riesgos, para obtener el resultado esperado por el sujeto obligado.
	Medios de acción	Hacer	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

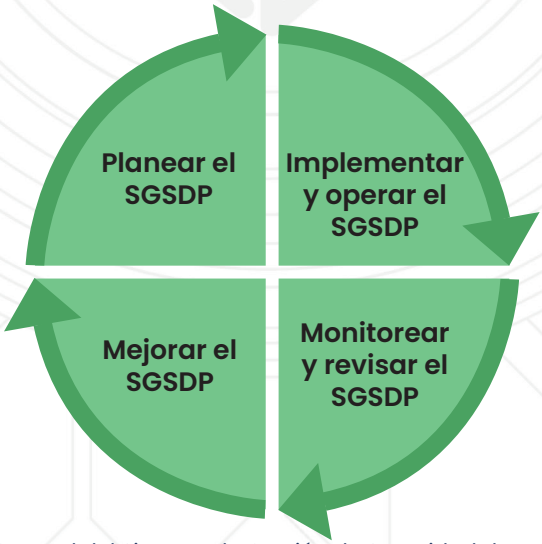


Figura 1. Ciclo General del Sistema de Gestión de Seguridad de Datos Personales
(Recomendaciones en materia de seguridad de datos personales, publicadas en el DOF el 30/10/2013.)

¿Qué es un riesgo?

De acuerdo con la Guía de apoyo para la elaboración del Documento de Seguridad[14], el riesgo es la combinación de la probabilidad de un evento y su consecuencia desfavorable.

Otra definición, retomada de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de información (MAGERIT) establece que un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización[15].

En otras palabras, es posible definir un riesgo a partir de la interacción de amenazas que atacan una o diversas vulnerabilidades de un activo o grupo de activos en perjuicio de la organización, en este caso de la entidad, por lo que, cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

¿Qué es la gestión del riesgo?

De acuerdo con el estandar internacional ISO 31000: 2018 -Gestión del riesgo- Directrices[16] la gestión del riesgo se refiere a la realización de actividades coordinadas para dirigir y controlar la organización con relación al riesgo, es decir, festionar el riesgo es realizar aquellas actividades necesarias para conocer el riesgo, comprenderlo y así poder tratarlo de acuerdo con las posibilidades y objetivos de la entidad.

El riesgo naturalmente genera incertidumbre respecto al cumplimiento de objetivos de cualquier entidad, en nuestro día a día las personas gestionamos el riesgo sin darnos cuenta, por ejemplo, comprendemos que para llegar de nuestro hogar a nuestro lugar de trabajo existe cierta probabilidad de que múltiples escenarios puedan materializarse y afecten nuestro objetivo, esto es, que lleguemos tarde al lugar de trabajo o que no lleguemos; en ese sentido, valoramos las múltiples amenazas de distinta índole, por ejemplo la inseguridad, el tráfico, un choque, e intentamos prevenir que nos afecten tomando ciertas medidas, por ejemplo, manejando con más precaución, elegimos la ruta más segura o más rápida, y salimos con antelación, previendo algunos de estos escenarios. Gestionar el riesgo es justamente esa comprensión del riesgo para mantenerlo controlado en la medida de lo posible a través de la toma de mejores decisiones.

El proceso de gestión de riesgos es iterativo, adaptable y continuo, el cual se adapta a las necesidades y el contexto de la organización, buscando mejorar de manera constante la capacidad de identificar, evaluar y tratar los riesgos de manera efectiva, partiendo de la idea general de que el riesgo cero no existe, alguna o algunas amenazas van a incidir en las vulnerabilidades de los activos

14 INAI, Mayo de 2024, Guía de apoyo para la elaboración del Documento de Seguridad. p13. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf

15 MAGERIT-versión 3.0, Libro I, Glosario. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

16 ISO/IEC 31000:2018, consulta realizada el 02/04//2024: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

de las Organizaciones, y se materializará el riesgo; ello puede retrasar o impedir el cumplimiento de sus objetivos; sin embargo, la gestión de riesgos se realiza también para prever el tratamiento del riesgo, con lo que se pueden tomar mejores decisiones para que ante dicha materialización, las consecuencias afecten lo menos posible.

En ese sentido, la gestión del riesgo enfocada a la seguridad de los datos personales en las organizaciones, lo que busca es comprender estos múltiples riesgos, a efecto de tratarlos, es decir, mantenerlos controlados en la medida de lo posible a fin de que podamos ejercer los objetivos, atribuciones y facultades que compete al sujeto obligado de una manera más eficaz y eficiente, y que ante la materialización del riesgo, se implementen medidas de seguridad y correctivas para reducir **las consecuencias negativas en los datos personales, en donde nos referimos a la posible vulneración de datos y a la intimidad de las personas, traduciéndose como una consecuencia no deseada, capaz de generar daños o perjuicios sobre las personas titulares**, **en sus derechos y libertades**.

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

El proceso de gestión de riesgos implica la aplicación sistemática de un proceso que se divide en:

- Establecer un alcance y describir un contexto respecto al trataiento de riesgos.
- Evaluar los riesgos a partir de (i) la identificación de los riesgos, (ii) el análisis de riesgos y (iii) la evaluación de los riesgos.
- Tratar los riesgos evaluados

Especificamente, al desarrollar el proceso de evaluación de riesgos es posible definir cada una de las actividades que comprenden esta etapa, primero, la identificación es la actividad en la que se identifican los eventos asociados con la pérdida de confidencialidad, integridad y disponibilidad de información en los activos de información identificados, el análisis de riesgos es comprender las consecuencias que pueden ocurrir si se materializasen los riesgos identificados, así como analizar la probabilidad de que los riesgos ocurran y valorar de forma cuantitativa y cualitativa el riesgo. La evaluación por su parte se refiere a comparar los resultados del análisis con los criterios de riesgo definidos en la metodología utilizada a fin de priorizar los riesgos que deben ser tratados.

Segundo, El análisis de riesgos como parte de la valoración del riesgo comprende otros procedimientos que son la identificación y la valoración de los activos, en este caso, los datos personales y sistemas del tratamiento; las amenazas que pueden afectarlos, las vulnerabilidades propias de los activos; asimismo debe identificarse de manera cuantitativa y/o cualitativa la probabilidad o la posibilidad de ocurrencia de que dichos escenarios hipotéticos se materialicen y la afectación que desencadenaría en los propios activos y en los titulares de los datos personales.

Tercero, la evaluación del riesgo es el proceso que apoya a la toma de decisiones. La evaluación de los riesgos implica comparar los resultados del análisis del riesgo con los criterios para riesgos establecidos para determinar cuándo se requiere una acción adicional que deriva en el tratamiento del riesgo.

Finalmente,el tratamiento del riesgo es la realización de actividades para manejar el riesgo a efectos de que, de materializarse, afecte lo menos posible en la consecución de los objetivos de la entidad, ello se hace a través de la toma de decisiones respecto al riesgo en estricto sentido, que pueden ser:

- Aceptar el riesgo
- Retener el riesgo,
- Transferir o compartir el riesgo,
- Reducir el riesgo,
- Evitar el riesgo

Una vez tomada la decisión sobre el tratamiento, deben implementarse las acciones y medidas de seguridad, controles o salvaguardas correspondientes para dicho fin.

Figura 2. Gestión de riesgo
Autoría propia

Por lo que, la gestión del riesgo comprende entonces primero la valoración del riesgo y posteriormente el tratamiento, en donde se busca:

1. Determinar qué activos tiene la organización y estimar lo que podría pasar.
2. Organizar de manera informada una serie de actividades preventivas evitando que ocurra un incidente, y, al mismo tiempo, se tenga un plan de acción y se esté preparado para una emergencia.

A continuación, se presenta un esquema del proceso de gestión de riesgos más exhaustiva, en materia de seguridad de la información.

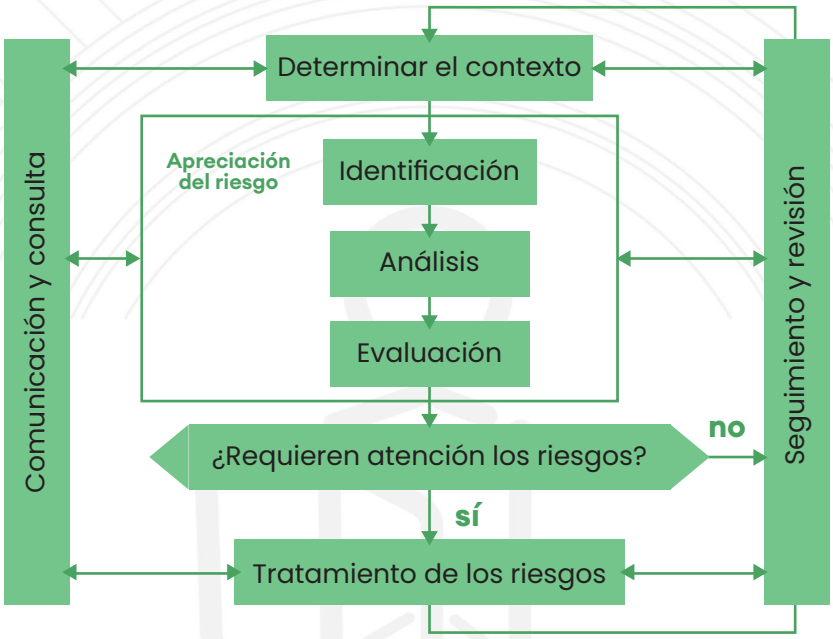


Figura 3. Diagrama MAGERIT basado en ISO 31000[17]

¿Cuál es la relación entre sistema de gestión y gestión de riesgos?

La relación entre un sistema de gestión particularmente de seguridad de la información es que utiliza el enfoque de la gestión del riesgo para la protección y seguridad de la información. En ese sentido, ubicando y comprendiendo el riesgo podemos implementar un sistema de gestión que abarque las acciones necesarias para operar la gestión del riesgo, y con ello proteger los activos de información de una organización, es decir del sujeto obligado; por ejemplo, mediante el monitoreo del riesgo y sus factores, hasta cómo implementar las propias medidas de seguridad, todo esto en un conjunto ordenado de acciones (sistema).
A efectos de consolidar un sistema de gestión de seguridad con un enfoque del riesgo, ya múltiples estándares internacionales comprenden en la propia implementación del sistema de gestión una metodología para la gestión del riesgo,

17 MAGERIT-versión 3.0, Libro I, Glosario. P. 20. Fecha de consulta: 02/04/2024 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

como en el caso de los estándares Internacionales de la Organización Internacional para la Estandarización (ISO) en conjunto con Comisión Electrotécnica Internacional (IEC), específicamente de la serie 27000, particularmente la 27001, la cual es una referencia para el cumplimiento de requisitos para la implementación de un sistema de gestión de seguridad de la información, refiriendo a la gestión del riesgo, sin embargo, es la 27005 la que consolida la metodología en este tema.

Existen estándares internacionales y marcos en materia de seguridad de la información y ciberseguridad, así como otras metodologías para la gestión de riesgos para la seguridad de la información, por lo que el sujeto obligado por sí mismo o mediante la contratación de consultoría externa podría implementar un SG, basándose en estándares, marcos nacionales e internacionales y metodologías, una vez implementado el SG, es posible buscar incluso alguna certificación internacional o bien un validación ante el Inai que puede culminar con el registro del Sistema de Gestión en el Registro de Esquemas de Mejores Prácticas (REMP)[18]. En la presente guía se propone un seguimiento de fases y pasos a fin de orientar a los sujetos obligados a la implementación de uno a efectos de que cumplan con el deber que mandata el artículo 34 de la Ley General.

Estándares internacionales sobre sistemas de gestión y metodologías de gestión de riesgos

Los estándares internaciones son creados con la finalidad de establecer mínimos referentes a ciertas materias, para orientar, coordinar y unificar criterios para las Organizaciones, dado el marco global en el que se desarrolla la economía actualmente, para efectos de brindar certidumbre en las interacciones entre organizaciones y terceros que busquen relacionarse con ellas.

El estándar por excelencia que contiene los mínimos para el establecimiento de un sistema de gestión de seguridad de la información como ya se mencionó es la ISO/IEC/27001; sin embargo, es la ISO/IEC/27005 la que contempla una metodología para la gestión del riesgo en materia de seguridad de la información.

Las metodologías para la gestión del riesgo por su parte se entienden como un conjunto de técnicas definidas y preestablecidas, empleadas para valorar los riesgos a los que se pueden enfrentar los datos personales y sistemas de tratamiento a efecto de tomar las mejores decisiones para salvaguardarlos. Se debe entender que en materia de seguridad de la información la metodología de ges-

18 Es común que las organizaciones quieran certificarse, sin embargo, no es un requerimiento para implementar un Sistema de Gestión, como tampoco para hacer una adecuada gestión de riesgos, sin embargo, al cumplir con un estándar y más aún con una certificación se brinda mayor certeza a otras entidades u Organizaciones que estén interesadas en contratar, o al público en general al que brinden su producto o servicio.
Respecto al Registro de Esquemas de Mejores Prácticas, se sugiere la lectura de la Guía de Mejores Prácticas en materia de Protección de Datos Personales con un enfoque práctico, disponible en https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Mejores-pr%C3%A1cticas_SP.pdf

tión de riesgos debe estar inmersa en la del sistema de gestión, ya que se requiere de una para su correcta implementación.

Cada responsable puede utilizar el estándar y la metodología que considere más conveniente, a partir del conocimiento de los activos que va a analizar, de esta manera, deberá tomar en cuenta que es posible adoptar y combinar elementos de diversas metodologías, según sea conveniente, incluso, si lo considera oportuno, podrá tratar de desarrollar una propia, siempre que ésta cumpla con los principios básicos que siguen todas las metodologías de gestión del riesgo, que sea congruente y esté documentada.

Por lo anterior, a la hora de elegir, hay que tener en cuenta que algunas de estas metodologías son más idóneas para las condiciones del análisis, además, se debe contar con bibliografía especializada y de ser posible con personal capacitado en la gestión de riesgos para la interpretación y aplicación de los contenidos.

En ese sentido y con el objetivo de brindar a los sujetos obligados un documento básico que oriente sobre los elementos y contenidos de manera general de las metodologías para la gestión de riesgo se efectuó una revisión genérica de los puntos clave de algunas y se tuvo como resultado lo siguiente:

Metodologías para la gestión del Riesgo

MAGERIT V3[19]	METODOLOGÍA BAA[20]	METODOLOGÍA PARA LA GESTIÓN DE RIESGOS SEGÚN ISO 31000:2018[21]	METODOLOGÍA CONFORME A LA NORMA ISO 27005[22]
La gestión de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados: • Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué	Esta metodología se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante: • Beneficio para el atacante. • Accesibilidad para el atacante. • Anonimidad del	El proceso propuesto por la ISO 31000 • **Comunicación y consulta:** Esta fase es importante dado que en ellas dan sus opiniones acerca del riesgo con base a la percepción de cada una de las partes involucra-	La norma ISO 27005 se define como el proceso de gestión de riesgo para la seguridad de la información basado en el ciclo PDCA (Plan- Do -Check- Act). • **Planear:** El establecimiento del contexto, valoración del riesgo,

19 Metodología MAGERIT, consta de 3 Libros, y se cuenta disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

20 Metodología BAA, creada por el INAI, disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_Análisis_de_Riesgo_BAA(Junio2015).pdf

21 ISO 31000, Prólogo y explicación de la norma, disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

22 Melo Reyes, Oscar Javier, Aspectos a tener en cuenta para el análisis de riesgos con base en las normas ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 31000. http://repository.unipiloto.edu.co/handle/20.500.12277/6350

perjuicio (coste) supondría su degradación.

- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué controles hay dispuestos y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

atacante.

A partir de lo anterior, se ha dado el nombre de "BAA" a esta metodología de análisis de riesgos. Los pasos en esta metodología son:

- Identificación y clasificación de datos personales.
- Clasificación de datos personales.
- Identificación de tipos de datos y de nivel de riesgo inherente.
- Análisis de riesgos de datos personales.
- Identificación de riesgo por tipo de dato.
- Identificación del nivel de riesgo por tipo de dato.
- Cuestionario de autoevaluación.
- Identificación de nivel de accesibilidad.
- Identificación de nivel de anonimidad.
- Identificación de nivel de riesgo latente.
- Identificación de medidas de seguridad.
- Tablas de control.
- Procedimiento de selección de medi-

das, la Comunicación y la consulta debe desarrollar planes que aborden aspectos del propio riesgo, sus causas y consecuencias (si se conocen), y las medidas que se tomen para tratarlo.

- **Establecimiento del contexto.**
  La organización articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso.
- **Valoración– identificación del riesgo:**
  El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar acelerar o retrasar el logro de los objetivos.
- **Valoración – análisis de riesgos:**
  La entrada de esta etapa es la lista de riesgos previamente identificados y el objetivo es desarrollar un entendimiento y comprensión acerca del riesgo y sus causas, utilizando como criterios la probabilidad de ocurrencia y el impacto de sus consecuencias, esto permite calcular el

comunicación del riesgo, aceptación del riesgo, comunicación del riesgo, monitorización y revisión del riesgo.

- **Hacer:**
  Se plantea el plan para el tratamiento de los riesgos. Descripción general de cómo se va a tratar el riesgo, reducción del riesgo, retención del riesgo, evitación del riesgo y transferencia del riesgo.
- **Verificar:**
  Monitoreo continuo y revisión de los riesgos previamente identificados en las etapas previas.
- **Actuar:**
  Mejora continua de la gestión del riesgo, con base en los resultados del monitoreo y revisión.

	das de seguridad. • Optimización de los niveles de riesgo. • Inventario de datos y sistemas de tratamiento. En resumen, los pasos a seguir son: • Identificar el riesgo por tipo de dato, de acuerdo con los datos personales que se tratan (nivel de riesgo inherente). • Con el número identificado en la primera tabla (nivel de riesgo inherente), se procede a buscar la tabla que le corresponde a ese número, para en ella utilizar como coordenadas las otras dos variables: accesibilidad y anonimidad. • Utilizando el grado de accesibilidad y anonimidad, es decir, desde dónde se accede a los datos (anonimidad) y qué cantidad de accesos existen (accesibilidad), se identifica la celda correspondiente en la cual se identificarán los patrones de controles que se requiere implantar.	nivel de riesgo en función de estas dos variables. El análisis del riesgo proporciona elementos de entrada para tomar decisiones sobre cuáles son los riesgos y las causas a los que se les debe dar un tratamiento inmediato, cuales admiten acciones a mediano plazo y cuáles pueden ser aceptados sin tener nuevas acciones, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados. • **Valoración: evaluación del riesgo:** Toma como entrada los resultados de la identificación y del análisis del riesgo y tiene como objetivo ayudar a la toma de decisiones, determinando los riesgos a tratar, la forma de tratamiento más adecuada para adaptar los riesgos adversos a un nivel tolerable y conocer la priorización para implementar el tratamiento determinado. • **Tratamiento de riesgos:** Involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. El tratamiento suministra control sobre	

		los riesgos o los modifica. • **Monitoreo y revisión:** Este proceso de monitoreo y revisión se ejecuta sobre los planes de tratamiento del riesgo y proporciona una medida del funcionamiento de estos, cuyos resultados, registrados en informes. • **Registro** Los registros brindan la base para la mejora de los métodos y las herramientas, así como del proceso global.	

Tabla 2. Comparativa de metodologías

Esta comparativa de metodologías se elaboró con fines didácticos sin intención de calificar o destacar cuál de ellas es mejor, se busca enfatizar las actividades principales de cada una a fin de que el sujeto obligado identifique si alguna le representa un mejor funcionamiento.

Dicho lo anterior, es importante que considere que cualquiera de las metodologías mencionadas para la gestión de riesgos requiere que el responsable destine recursos materiales, financieros y humanos, orientados a la especialización en la gestión de riesgos de aquellos que realicen esta actividad a fin de llevar a cabo una correcta implementación de un Sistema de Gestión de Seguridad de Datos Personales en función de la gestión del riesgo.

Por lo expuesto, este documento no pretende determinar qué metodología es más adecuada, ya que se debe partir de que todas tienen el mismo objetivo, adicionalmente de la comparación se pueden identificar puntos en común o pasos a seguir, los cuales conformarían una base mínima para la gestión del riesgo y para la implementación de un Sistema de Gestión.

Para la elaboración del presente documento se tomaron como base el estándar ISO/IEC/27001 en conjunto con múltiples metodologías de gestión de riesgo como ejemplo, Marco de Gestión de Riesgos del Marco de Seguridad NIST de Estados Unidos de América Risk Management Framework[23], la Guía de Gestión de Riesgos y Evaluaciones de Impacto de la Agencia Española de Protección de Datos[24], la Guía de Gestión de riesgos del Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador[25], la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT versión 3.0[26] elaborada por el antiguo Consejo Superior de Administración Electrónica del Gobierno de España que actualmente es mantenida por la Secretaría General de Administración Digital con la colaboración del Centro Criptológico Nacional.

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 consideran diferentes pasos y objetivos específicos para el SGSDP, que pueden observarse en la siguiente tabla:

Ciclo	Fases		Pasos	Objetivos Específicos	Recursos, documentación del sistema, sensibilización y capacitación (procesos transversales, aplican en todas las fases del ciclo)
	Planificar	Planear el SGSDP	1. Alcance, objetivos, contexto y establecimiento de criterios para la gestión y tratamiento del riesgo. 2. Política de gestión de datos personales. 3. Funciones y obligaciones de quienes traten datos personales.	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para **gestionar los riesgos de los datos personales, con el fin de proteger los datos personales de los titulares, cumplir la Ley en la materia** y obtener resultados acordes con las políticas y objetivos generales del sujeto obligado.	

23 Disponibles múltiples guías en: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

24 Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

25 Metodología disponible en: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/12/Acuerdo-Ministerial-No.-025-2019-EGSI-Versi%C3%B3n-2.0_compressed.pdf

26 Metodología disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

			4. Identificación de tratamientos-Inventario de datos personales. 5. Gestión de los riesgos de los datos personales: análisis, evaluación y tratamiento (análisis de brecha).	
	Hacer	Implementar y operar el SGSDP	6. 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	7. Revisión de los factores del riesgo. 8. Evaluación de la eficacia de las medidas de seguridad. 9. Auditorías. 10. Revisión por el Comité y Directivos.	Evaluar y medir el cumplimiento del proceso y su eficacia de acuerdo a los objetivos planteados para el sistema de gestión y de acuerdo con la legislación de protección de datos personales, la política, los objetivos y la experiencia práctica del SGSDP, e informar los resultados al Comité de Transparencia y los Directivos correspondientes para su revisión y mejora.
	Actuar	Mejorar el SGSDP	9. Mejora continua.	La mejora continua es aprender de los resultados de monitoreo y revisión e implementar actualizaciones y cambios para un mejor funcionamiento del sistema mediante acciones preventivas y correctivas. aprender de ellas.

Recursos, documentación del sistema, sensibilización y capacitación (procesos transversales, aplican en todas las fases del ciclo)

Tabla 3. Objetivos del SGSDP dentro de las fases del ciclo PHVA Recomendaciones en materia de seguridad de datos personales, publicadas en el DOF el 30/10/2013.

Al interior de los sujetos obligados los procesos deberían ser documentados y en ellos se involucra 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.

Para la Ley General y sus Lineamientos, los datos personales son el principal activo de información, el artículo 33, de la Ley General y el Capítulo II de sus Lineamientos Generales, vislumbran que una de las primeras acciones para protegerlos es tener bien identificado, definido y documentado el flujo de los datos personales que se traten a través de los diferentes procesos del sujeto obligado.

Asimismo, durante el ciclo del SGSDP se deben identificar y valorar 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. Implementación del Sistema de Gestión de Seguridad de Datos Personales conforme al ciclo PHVA o ciclo Deming

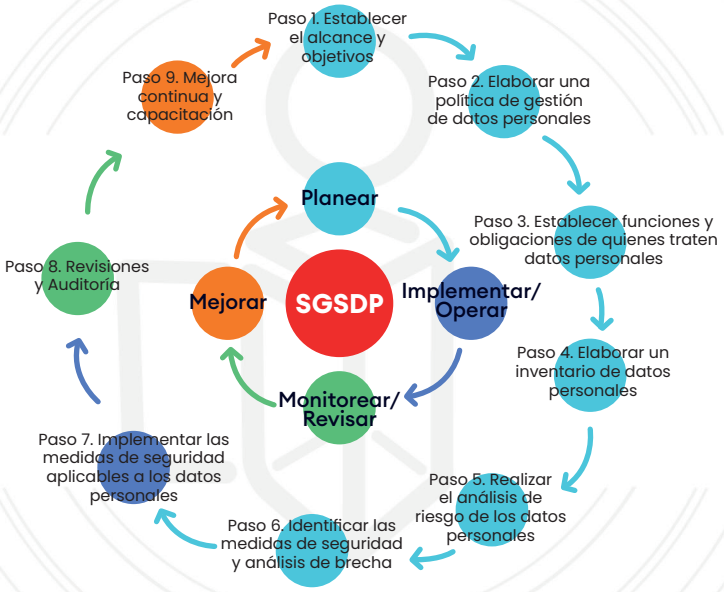


Figura 4. Ciclo de un Sistema de Gestión de Seguridad de Datos Personales: Fases y pasos de cada fase. Autoría propia

Es importante señalar que, si bien para efectos de orientación se establecen los pasos a seguir para la implementación del SGSDP, estos no deben considerarse como un flujo de acciones inamovibles que deben finalizarse para pasar a la siguiente acción, ya que se trata de un ciclo de mejora continua, por lo que muchos de los pasos se consolidarán en distintas fases, e incluso en diversas iteraciones del ciclo, y como se observará en la fase dos, existen procesos transversales que deben implementarse durante todas las fases.

Por ejemplo, de acuerdo con la figura anterior, el paso 2 señala establecer las políticas de gestión de seguridad de la información, si bien, la Política General puede consolidarse ya que se trata de plasmar los objetivos, bases y principios

generales que regirán el actuar del sujeto obligado en materia de protección de datos personales, las políticas técnicas complementarias, difícilmente podrán estar consolidadas desde ese momento, ya que se requerirá realizar el análisis de riesgos y la planeación de su tratamiento para definirlas, y deberán estar en constante revisión y actualización para su mejora.

Fase 1. Planear el Sistema de Gestión de Seguridad de Datos Personales

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 el sujeto obligado, 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 los **objetivos del SGSDP de acuerdo al contexto** del sujeto obligado, fijar el **alcance del SGSDP**, definir la **metodología para la gestión y tratamiento del riesgo y los criterios mínimos**;
2. Elaborar la **Política General de Gestión de Datos Personales**.
3. **Identificar los activos de información que contienen datos personales, y los sistemas del tratamiento** que los soportan, contienen y mediante los que se transmiten, a través de la elaboración de un **inventario de datos personales y sistemas de tratamiento;**
4. **Establecer las funciones, obligaciones, roles y responsabilidades de quienes traten los datos personales**;
5. **Analizar los riesgos** a los que están sujetos los datos personales y sistemas de tratamiento,
6. **Identificar las medidas de seguridad** a implementar, realizando el análisis de brecha
7. Documentar la planeación de la implementación de las medidas de seguridad en **un plan de trabajo.**

Paso 1. Establecer los objetivos del Sistema de Gestión de Seguridad de Datos Personales de acuerdo con el contexto del sujeto obligado, fijar el alcance, definir la metodología y criterios para la gestión del riesgo

Paso 1.1 Definir el alcance y los objetivos del Sistema de Gestión de Seguridad de Datos Personales de acuerdo con el contexto del sujeto obligado

Analizar el contexto de la entidad es indispensable pues se requiere comprender a profundidad al sujeto obligado para saber el objetivo y alcance del SGSDP, es decir ¿qué vamos a proteger?

Es necesario conocer los objetivos del sujeto obligado, entiéndase sus funciones y atribuciones para cumplir con el mandato constitucional o legal correspondiente, y sus procesos internos, así como a las partes interesadas, por ejemplo, los gobernados titulares de datos personales, los empleados, y externos que pueden afectarle en su operación como contrataciones con terceros y demás autoridades con las que interactúa, así como con los procesos internos de la entidad, y sus expectativas. Es decir, es importante conocer a las partes interesadas, así como el entorno que puede generar incertidumbre respecto al cumplimiento de los objetivos de la entidad, como pueden ser financieros, las leyes y regulaciones existentes, condiciones culturales, económicas, geográficas y ambientales, sí como las contrataciones con terceros.

Para ello, previo a la definición del alcance y los objetivos, debe analizarse el tipo y tamaño del sujeto obligado, las Unidades Administrativas que lo conforman y su contexto interno y externo.

Respecto al contexto externo se deben considerar los siguientes factores:

- Factores legales y regulatorios: se reflejan en leyes nacionales y locales o acuerdos internacionales, así como en la regulación secundaria. Por ejemplo, la Ley General y sus Lineamientos Generales, leyes de protección al consumidor, leyes de notificación de vulneraciones, leyes laborales, entre otras.
- Factor contractual o de relaciones con terceros: 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.
- Factor político: reflexionar por ejemplo sobre si la seguridad de la información y los datos personales están siendo parte de la agenda pública, lo que realizan las autoridades de control en materia de protección de datos personales.
- Factor social: se debe analizar cómo está respondiendo la sociedad o los cambios sociales que tienen que ver con la seguridad de los datos personales, por ejemplo, si se está socializando el derecho a la protección de datos personales, o si los titulares están presentando solicitudes para el ejercicio de derechos ARCO.
- Factor económico: de igual forma debe estudiarse la incidencia que pueda tener la economía en el sujeto obligado y particularmente en materia de seguridad de los datos personales.
- Factor tecnológico: se debe analizar cómo está afectando o incidiendo los avances tecnológicos en el derecho a la protección de datos personales y a su seguridad.

Respecto al contexto interno se deben tomar en cuenta factores como:

- El estilo y los valores compartidos por el sujeto obligado: el estilo se refiere a la cultura de la organización y los valores compartidos son el corazón de la organización, sus principios y filosofía que lo guía.
- El personal: los recursos humanos son un activo fundamental en las organizaciones, y su labor debe estar orientada hacia la estrategia y cum-

pliendo el estilo y los valores definidos.
- Las habilidades y competencias con las que cuenta el personal: se refiere a las habilidades y conocimientos con los que cuenta tanto el personal como los directivos, es decir todos los miembros de la organización.
- Los sistemas: son los procesos internos que definen los parámetros de funcionamiento de la entidad y los sistemas de información son los canales por los que transita la información.
- La estrategia de trabajo: se trata de la forma de enfocar y manejar los recursos para conseguir los objetivos de la entidad.
- La estructura: se refiere a la forma en que se organiza el propio sujeto obligado, como se relacionan e interactúan las distintas unidades administrativas.

Todo lo anterior, respecto al enfoque de seguridad de los datos personales y la gestión del riesgo.

Una vez analizado el contexto, se deben definir los objetivos y el alcance del SGSDP. Definir el alcance y objetivos se refiere a delimitar el sistema de gestión, esto es, identificar las áreas, procesos, sedes, en su caso, que son relevantes y que se deben proteger en tanto que en ellos se procesan datos personales, para que respecto de ellos se implemente dicho sistema.

Por ejemplo, el alcance y delimitación para la implementación del sistema de gestión, pueden ser una aplicación de tecnología de la información, infraestructura de tecnología de la información, un proceso del negocio o una parte definida de la institución, y los objetivos son la protección adecuada de los datos personales y activos de información que los contienen que interactúan en los procesos institucionales en cumplimiento de la LGPDPPSO y de los LGPDPSP.

Debe quedar claro, que el objetivo final y el alcance por mandato legal, debe comprender todos los procesos y unidades administrativas en los que se lleven a cabo tratamientos de datos personales en el sujeto obligado, sin embargo, dada la complejidad de la implementación, en cuanto a trabajo, y recursos administrativos, humanos, económicos, etcétera, en primera instancia, puede reducirse el alcance, por ejemplo, a los procesos que involucren tratamientos de datos personales más críticos, y con el paso de iteraciones del SGSDP, es posible ir ampliando el alcance hasta que toda la organización (todas las unidades administrativas que traten datos personales) se encuentren dentro del alcance del SGSDP.

Así, una vez entendiendo y conociendo el contexto del sujeto obligado en materia de protección de datos personales y su seguridad, se podrá delimitar el alcance del SGSDP, esto es, a los sistemas de tratamiento y las unidades administrativas que traten datos personales en cualquier fase de su ciclo de vida, además de que se podrán establecer los objetivos de seguridad que se buscan con su implementación.

Paso 1.2. Definir la metodología y criterios mínimos de la gestión de riesgos

Posterior a la definición del alcance y objetivos, se debe **establecer la metodología de gestión de riesgos que se utilizará**, así como **los criterios básicos para la gestión y evaluación del riesgo**, que permitan tomar mejores decisiones para el tratamiento de los riesgos.

Es indispensable que estos se definan en este paso, y previo al análisis y valoración del riesgo a efecto de poder obtener resultados objetivos, consistentes y comparables, ya que como se señaló en el punto 2.2. Conceptos clave para comprender un Sistema de Gestión de Seguridad de Datos Personales, la gestión de riesgos y la gestión de la seguridad de los datos personales es un proceso de mejora continua que requiere actualización constante, lo que implica la realización iterativa de la valoración del riesgo (identificación, análisis y evaluación del riesgo) en ese sentido, la fijación de los criterios es a efectos de que los resultados sean comparables con las siguientes iteraciones, a fin de observar si se está tratando el riesgo conforme a los objetivos de seguridad y los criterios planteados.

Para efectos de lo anterior, deberán definirse escalas de valor ya sea cualitativas, cuantitativas o mixtas. Las escalas cualitativas se utilizan cuando la información que se tiene es subjetiva, por ejemplo, cuando no se tiene claro el valor numérico que representa para la entidad un activo en particular o por ejemplo cuando no se tienen registros para el criterio de probabilidad, es decir, cuántas veces en un periodo de tiempo se ha materializado un suceso, la frecuencia; sin embargo, en este caso, en las siguientes iteraciones podrá conjuntarse información y por lo tanto se podrán realizar registros, para establecer una escala de valores cuantitativos. Cuando no se tienen registros, será importante allegarnos de información del entorno y quizá opiniones de expertos que nos den pautas para establecer la probabilidad.

Las escalas cuantitativas por su parte, es cuando se cuenta con información objetiva, por ejemplo con información estadística y con registros que indiquen la posibilidad de que un evento ocurra.

Las escalas mixtas, son las que combinan ambas escalas, ya que habrá elementos donde contemos con datos objetivos y registros, y en otros casos no, por lo que tengamos que usar un criterio subjetivo, asimismo, aunque tengamos registros e información subjetiva, es recomendable establecer escalas de valor mixtas. Para efectos de los ejemplos vertidos en la presente guía se utilizarán escalas de valor mixtas.

Ahora bien, es posible que "se establezcan criterios para todos los componentes del riesgo (…)"[27] por ejemplo, para definir quienes serán los propietarios del activo que contiene los datos personales, el propietario del riesgo, criterios para

27 Corona Fraga, Pablo. Guía Práctica para la gestión de los riesgos en la era de la ciberseguridad. P.60

la aceptación del riesgo o el nivel de riesgo aceptable, los criterios para la valoración de los activos, los criterios de la probabilidad, los del impacto entre otros.

Para efectos de realizar una gestión del riesgo sencilla y que oriente y facilite la elaboración de un Sistema de Gestión de Seguridad de Datos Personales, se recomienda por lo menos establecer los criterios de Nivel de Riesgo Aceptable (NRA), los criterios de valoración de los activos, los de probabilidad y los criterios de impacto en los activos y en los titulares de los datos personales, así como los factores que señala el artículo 32 de la LGPDPPSO[28].

- **Nivel de Riesgo Aceptable (NRA)**

En este punto deberá fijarse el criterio sobre el NRA, este se refiere al nivel en una escala cuantitativa y cualitativa que será el máximo riesgo para aceptar dentro de la entidad, esto se debe fijar a través de considerar los criterios y parámetros que exige la Ley General, y de manera general a los niveles de riesgo que un sujeto obligado se fije como meta respecto a sus alcances y objetivos.

Ahora bien, si lo que se busca es salvaguardar los datos personales para a su vez proteger la vida, integridad, derechos y libertades de las personas titulares, se recomienda que, el nivel de riesgo aceptable sea un riesgo bajo o muy bajo (depende de la escala cuantitativa y cualitativa establecida), sin embargo, en caso de que el sujeto obligado considerara, por cuestiones del contexto de la entidad, de los recursos humanos, administrativos y económicos, aceptar o retener un riesgo mayor, es decir medio o alto, (no se recomienda en ningún caso aceptar un riesgo alto o muy alto) deberá ser acordado y aceptado formalmente por el Titular de la unidad administrativa correspondiente o propietario del Tratamiento y/o activo, en conjunto con el Comité de Transparencia, y si es posible incluso por los Órganos de Gobierno o Directivos del sujeto obligado, debiendo especificar las acciones a implementar para su monitoreo o futura implementación de medidas de seguridad para tratarlo. Esta recomendación obedece a lo dispuesto en la fracción V, del artículo 84 de la LGPDPPSO.

- **Los criterios para la valoración de los activos**

Se deben establecer criterios que permitan asignar valor a cada activo en relación con su función en la entidad, es decir, se debe buscar el beneficio que trae dicho activo para la operación del sujeto obligado, por ejemplo, si es un habilitador para llevar a cabo procesos sustantivos o administrativos fundamentales, y por lo tanto su valor estará definido por el beneficio que aporta para el cum-

28 Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:
I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. 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.

plimiento de los objetivos (facultades y atribuciones) que tiene encomendado el sujeto obligado.

Será importante que se establezca una escala cualitativa y/o cuantitativa para su valoración siendo recomendable también, que se valoren en las tres dimensiones o propiedades de seguridad de la información (confidencialidad, integridad y disponibilidad).

Existen múltiples metodologías para la valoración de activos, es posible que se realicen a través de un árbol de dependencias como lo sugiere MAGERIT 3.0 donde se deben clasificar y valorar los procesos a nivel macro de la entidad e ir mapeando los activos de información de los que dependen dichos macroprocesos, estos activos irán heredando la valoración de los activos previos y los procesos que soportan.

En la presente guía se propone un criterio más sencillo que es cuestionar de manera subjetiva la valía que tiene el activo en cada propiedad de seguridad de la información y posteriormente se sumará su valor. (Ver ejemplo en el paso 5. Gestión de riesgos)

Valorar los activos es indispensable para entender cuál es su criticidad e importancia dentro del sujeto obligado, a fin de que en el análisis de riesgos y en el tratamiento de riesgos se le brinde la prioridad correspondiente a los activos más importantes o críticos.

- **Los criterios de impacto y probabilidad**

El impacto son aquellas consecuencias negativas que son resultado de la materialización del riesgo, es decir, son las consecuencias que tiene la vulneración de los activos materializado en la entidad y en el titular de los datos personales.

En este caso relativo a los datos personales como activo de información o activo principal y en el sentido de que el derecho a la protección de datos personales se trata de un derecho fundamental, debe analizarse el impacto en términos del daño que genera una vulneración en los activos y operación de la entidad pero que a su vez genera afectaciones a las personas titulares de los datos personales, esto es, en primera instancia los daños al propio activo como puede ser un sistema de tratamiento, que pueda afectar incluso la operación del sujeto obligado, y que a su vez cause la pérdida o afectación de los datos personales y por lo tanto genere daños o afectaciones a las personas titulares.

En ese sentido, si bien se debe analizar la afectación a la organización o al sujeto obligado, en sus recursos y su reputación, que importa y afecta, no es el fin último y propósito del sistema de gestión de seguridad de los datos personales, en tanto que este representa el deber de seguridad que tienen los sujetos obligados como responsables del tratamiento de proteger en primera instancia a las personas titulares, de los riesgos y amenazas a sus datos personales. Por lo que al valorarse el impacto a los datos personales y por lo tanto a las personas titulares,

deben considerarse, por ejemplo, sin ser este limitativo:

I. Daños o riesgos físicos en su persona e integridad.
II. Daños a su salud física o mental
III. Discriminación o alguna vulneración de sus derechos fundamentales.
IV. Daño moral
V. Daño patrimonial

Para ello se deberá establecer una escala cuantitativa, cualitativa o mixta donde se deberá valorar en dicha escala el impacto que pueda tener una vulneración en los activos con respecto a las tres dimensiones de seguridad:

- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de la información de completitud y exactitud.
- Disponibilidad: propiedad de la información de ser y estar accesible y utilizable a petición de una entidad autorizada.

Y se deberá analizar las afectaciones al sujeto obligado y a los titulares de los datos personales, finalmente se recomienda obtener un resultado único para el impacto.

Será importante que en la valoración por cada dimensión de seguridad sea en el mismo rango cuantitativo que el impacto en sí mismo.

$$impacto\ total = \frac{\text{confidencialidad} + \text{integridad} + \text{disponibilidad}}{3}$$

Figura 5. Propuesta de fórmula para el impacto

La escala y los criterios del impacto deben quedar fijados en esta etapa, aunque se aplicarán hasta el análisis de riesgos como parte de la gestión de estos, como se observa en el Paso 5. Gestión de Riesgos, donde se pueden observar ejemplos.

El criterio de probabilidad se refiere a la posibilidad de ocurrencia de un hecho o acontecimiento, considerando la cantidad de veces que podría presentarse en determinado periodo de tiempo, basándose en las eventualidades conocidas y el conocimiento del entorno, o bien a través del juicio de una persona experta.

En este caso deberá valorarse en una escala temporal recomendablemente traducida a una cuantitativa y cualitativa, la frecuencia de ocurrencia de que las amenazas vulneren los activos que contienen datos personales. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico del sujeto obligado, por ejemplo, bitácoras de incidentes y registros históricos, en caso de no contar con ellos, primero, será importante comenzar a elaborarlos, y segundo, se podrá elaborar a través de opiniones de expertos (datos subjetivos) o bien, de otros factores como de observar factores internos y externos

que pueden propiciar la aparición u ocurrencia del riesgo, aunque este no se haya materializado anteriormente, por ejemplo, el contexto externo: cambio de leyes, eventos naturales-ambientales, entre otros; del contexto interno: cambio en los procedimientos, falta de capacitación, ausencia de recursos tecnológicos; el compromiso del personal, la ética y cuidado con el que desempeñe sus actividades, el nivel de participación, entre otros.

La escala y los criterios de la probabilidad deben quedar fijados en esta etapa, pueden utilizarse los mencionados como ejemplo en el Paso 5. Gestión de Riesgos.

- Los factores del artículo 32 de la LGPDPPSO. El sujeto obligado deberá incorporar como factores de criticidad en la metodología, los enunciados en el artículo 32 de la LGPDPPSO.

Artículo 32 de la Ley General:
Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. 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.

El sujeto obligado deberá incluir en su gestión y análisis de riesgos los factores del artículo 32, en tanto que, de ello, dependerá las medidas de seguridad que implemente y su robustez; estos factores deben analizarse a fondo y revisar si pudiesen aumentar la criticidad de la posible materialización de un riesgo, por cuanto a la probabilidad o si incide en el impacto o consecuencia desfavorable a las personas titulares.

1. Riesgo inherente. se trata de la obtención del valor de riesgo intrínseco al activo el cual deriva de la aplicación de la metodología de gestión de riesgos.
2. La sensibilidad de los datos tratados. Es un factor que podría aumentar el impacto en las personas titulares, en tanto que la vulneración de datos sensibles puede traer consecuencias muy graves a las personas. Se debe comprender que la criticidad del activo es más alta cuando se tratan datos sensibles como pueden ser de salud, antes que un activo que solo almacene datos de identificación.
3. Desarrollo tecnológico. De igual forma, las amenazas y vulnerabilidades de los activos no serán las mismas si se trata de un sistema físico, que un sis-

tema electrónico y que además implique desarrollo de nuevas tecnologías.

4. Las posibles consecuencias de una vulneración para las personas titulares. Se refiere meramente al impacto en las personas titulares en caso de materialización del riesgo.
5. El número de titulares. Se debe tener presente que las medidas de seguridad deberán ser más robustas si se poseen datos de más personas titulares, eso no quiere decir que las pequeñas bases de datos que contienen datos de pocas personas titulares no se resguarden, sin embargo, estos factores ayudan a mirar la perspectiva y a priorizar la seguridad de los activos y tratamientos más críticos.
6. Las vulneraciones previas ocurridas en los sistemas de tratamiento. Se refiere al análisis de los criterios de probabilidad de que un riesgo se materialice en un periodo de tiempo y por las condiciones o el contexto.
7. 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. Se refiere al beneficio cuantitativo o cualitativo que pudiese obtener el tercero no autorizado que vulneró los datos personales o quien los recibió y puede aprovecharlos derivado de la vulneración.

Paso 2. Elaborar una Política de Gestión y Tratamiento de Datos Personales

Una vez que han sido definidos los alcances y objetivos de la gestión de los datos personales, el responsable deberá emitir e implementar una política general de gestión y seguridad de datos personales que ayude al logro de los objetivos planteados.

Además, de lo anterior 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 del sujeto obligado, 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 definido su alcance y objetivo, y recordar que esta debe aplicar a todos los servidores públicos que traten datos personales, así como a todos los datos personales que son tratados en el sujeto obligado dentro de los distintos procesos que lleva a cabo. Dicha política debe ser formalmente aprobada, coordinada y supervisada por el Comité de Transparencia conforme al artículo 47 de los Lineamientos Generales, y debe hacerse del conocimiento, y ser apoyada por Órganos de Gobierno u Órganos Directivos, de la entidad, asimismo para efectos de un Sistema de Gestión es importante considerar que las políticas tanto generales como técnicas complementarias, deben ser elaboradas por un equipo multidisciplinario dentro del sujeto obligado, que debe estar coordinado por el Comité de Transparencia, ello en razón de que se requerirá plasmar en ellas conceptos sobre protección de datos personales, pero también

respecto a medidas de seguridad administrativas, físicas y técnicas de distintos activos por lo que se requerirá de múltiples conocimientos desde jurídicos hasta de seguridad física y tecnológicos para su correcta elaboración.

Debemos recordar que la elaboración de políticas en materia de protección de datos personales es además de una parte fundamental del SGSDP, una medida para el cumplimiento del principio de responsabilidad de acuerdo con el artículo 30, fracciones I y II de la LGPDPPSO.

Artículo 30 de la Ley General:
Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

IX. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;

X. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;

(...)

Asimismo, representan un deber conforme al artículo 33, fracción I:

Artículo 33 de la Ley General:
Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
(...)

Y, a su vez son una medida de seguridad administrativa como lo señala el artículo 3, fracción XXI.

Artículo 3 de la Ley General:
Artículo 3. Para los efectos de la presente Ley se entenderá por:
(...)

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
(...)

Lo anterior, no quiere decir que se requiera una política por cada ocasión que la Ley las mencione, lo que se busca es que exista una o varias políticas generales que establezcan las bases y principios del actuar de todas las personas internas o externas a la entidad, traten datos personales de los que el sujeto obligado sea responsable, y de esta o estas deriven las políticas técnicas complementarias que se requieran de acuerdo con las necesidades y el contexto del sujeto obligado. Con dicho compendio de políticas se estaría cumpliendo el principio de responsabilidad, el deber conforme al artículo 33 de la Ley, y estas deben estar integradas y documentadas dentro del SGSDP y por lo tanto también se verán reflejadas en el Documento de Seguridad.

Al respecto, se recomienda revisar el documento Recomendaciones para la elaboración de políticas internas de gestión y tratamiento de datos personales (Sector Público)[29]

En el caso particular del paso 2 del SGSDP se refiere particularmente a la o las políticas generales, las cuales deben establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento de datos personales, por lo que debe ser comunicada a los mismos, e incluir al menos las siguientes reglas de acuerdo con lo establecido en el artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público:

Artículo 56 de los Lineamientos Generales:
Artículo 56. Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente:

I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales;

II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;

III. Las sanciones en caso de incumplimiento;

IV. La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;

V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y

VI. El proceso general de atención de los derechos ARCO.

29 Disponible en https://home.inai.org.mx//wp-content/documentos/Do- cumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf.

Deberán considerarse de manera general todos los principios que constan en los artículos 16 a 30 de la LGPDPPSO, desarrollados en los artículos 7 a 54 de los Lineamientos generales, y los deberes contenidos en los artículos 31 a 42 de la misma Ley, desarrollados en los artículos 55 a 72 de los Lineamientos Generales.

Paso 3. Identificar los tratamientos de datos personales, los activos que los contienen, procesan, almacenan y transmiten, así como los sistemas de tratamiento, y documentarlos en un inventario de activos

En este paso se busca documentar un listado de todos los sistemas de tratamiento físicos y electrónicos en donde se efectúe tratamiento de datos. Esta parte del sistema de gestión de seguridad de datos personales se relaciona con la elaboración del inventario de datos personales y sistemas del tratamiento a que refiere la fracción III del artículo 33 y fracción I del 35, ambos de la Ley General. Respecto al 33, fracción III, para el sistema de gestión y en particular, respecto a la gestión del riesgo, es la primera actividad que debe realizarse para la valoración del riesgo, y respecto al artículo 35, fracción I, es el primer contenido del Documento de Seguridad, por lo que los sujetos obligados podrán utilizar este último, en caso de que ya lo tengan elaborado, para identificar los activos que contienen datos personales, y los sistemas de tratamiento y someterlos al análisis de riesgos y al análisis de brecha, así como para el sistema de gestión.

Importante
La identificación de los activos es un punto clave en un sistema de gestión de seguridad de datos personales, puesto que es la base para la identificación de las amenazas, vulnerabilidades, y determinar el nivel de riesgo y exposición de los activos a este, y para la selección de controles para mitigarlos.

Un activo se define, de acuerdo con la Guía Gestión del Riesgo y Evaluación de Impacto en tratamientos de datos personales, de la Agencia Española de Protección de Datos, como "*todo bien o recurso que puede ser necesario para implantar y mantener una operación de tratamiento de datos personales en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada del tratamiento.*"[30]

En ese sentido, los activos que tienen valor y requieren resguardarse son los datos personales, recordando que estos activos conviven con otros activos como lo son: servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
De esta manera, se pueden identificar dos tipos de activos:

30 AEPD, (2021, junio), Gestión del riesgo y evaluación de impacto en tratamiento de datos personales. Fecha de consulta: 02/04/2024. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

- Activos de información: que son los datos personales.

- Activos de apoyo: que son los elementos físicos e infraestructura que soporta los activos de información, por ejemplo:
  - Hardware
  - Software
  - Redes y telecomunicaciones o personal
  - Estructura organizacional.
  - Infraestructura adicional.

Los activos deben estar identificados primero en el tratamiento a efectos de que en el inventario se plasme el flujo de los datos dentro de los procesos del sujeto obligado y los activos de soporte en los que se almacenan y transmiten, así como su ciclo de vida.

Es de señalarse que uno de los pasos del Documento de seguridad es el inventario, por lo que en caso de que el sujeto obligado haya avanzado en el cumplimiento al artículo 35 de la Ley General, contará con este insumo de lo contrario deberá elaborar un inventario de datos personales y de los sistemas de tratamiento conforme a lo dispuesto en la Ley General y en los Lineamientos Generales, atendiendo lo siguiente:

Artículo 33 de la Ley General:
"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. (...)

II. (...)

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento"

Artículo 58 de los Lineamientos Generales:
"Inventario de datos personales
Artículo 58. Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:
I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y
VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Artículo 59 de los Lineamientos Generales:
"Ciclo de vida de los datos personales en el inventario de éstos
Artículo 59. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:
I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales.
El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

Importante
Es obligación de los sujetos obligados mantener actualizado un inventario de los sistemas de tratamiento de datos personales que utiliza una organización, por lo que, es necesario involucrar a cada área que realiza el tratamiento pues ellos son los que identifican el tratamiento a declarar.

Dicho inventario debe identificar o estar vinculado con la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales, información que se relaciona de manera directa con su flujo o ciclo de vida considerando su:

- 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 6. Ciclo de vida de los datos personales.
Autoría propia

El inventario de datos es parte de las acciones encaminadas a garantizar la seguridad de los datos personales, por lo que se puede entender como el control documentado que se llevará de los tratamientos que realizan las áreas de la organización y los activos de información que contienen datos personales, realizado con orden y precisión.

Los elementos mínimos por considerar para el inventario de datos personales y sistemas de tratamiento deben contestar a las siguientes preguntas:

1) **¿Qué fundamento jurídico y atribuciones de la unidad administrativa identifica para realizar el tratamiento?**

Antes de iniciar el inventario es necesario identificar el fundamento jurídico que habilita el tratamiento y las atribuciones de la unidad administrativa que la facultan para realizarlo.

Asimismo, además de las facultades legales, debe identificar el fundamento ju-

rídico señalado en la Ley General, que legitima el tratamiento, esto es o bien el consentimiento, o alguna de las excepciones a éste, mencionadas en las fracciones del artículo 22.

2) ¿Qué tipo de datos personales recabo?
Para identificar qué tipo de datos personales se recaban en los distintos formatos que se utilizan y lo más importante preguntarse, si es necesario recabarlos o no. Esto con el fin de utilizar sólo los necesarios para el ejercicio de sus funciones.

3) ¿Cómo recabo esos los datos personales?
Para identificar en qué tipo de formatos se recaban y almacenan los datos personales por el responsable.

4) ¿Dónde se almacenan los datos personales?
Cada formato identificado puede estar almacenado en una o más ubicaciones, físicas o electrónicas.

5) ¿Quién tiene permiso para acceder o manejar los datos personales?
Diferentes personas pueden tener acceso a los sitios donde se almacenan los datos personales, estás pueden tener permisos específicos.

Para obtener mayor detalle en su inventario de datos personales, podrá ir atendiendo los contenidos que se consideran en las siguientes secciones:

Identificar a la unidad administrativa que declara el sistema de tratamiento de datos personales
En esta sección se deberá identificar puntualmente la información concerniente a la unidad administrativa que está declarando el sistema de tratamiento, por lo que se contemplan los siguientes indicadores para llenar:

- Nombre de la unidad administrativa
- Fecha de elaboración
- Fecha de última actualización
- Nombre del tratamiento
- Fundamento jurídico que habilita el tratamiento
- Atribuciones de la unidad administrativa para realizar el tratamiento

- ¿Qué tratamientos de datos personales realiza la unidad administrativa?

Se debe identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

- ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos, y cuales son usuarias o tienen acceso a esa misma base de datos?

Hay que identificar o definir si la unidad administrativa está a cargo del proceso

en donde se tratan los datos personales, según las atribuciones o facultades normativas, así como ver la interacción de otras Unidades administrativas en un mismo tratamiento, o en varios.

Por ejemplo, un sujeto obligado cuenta con una Dirección de reclutamiento y otra de Administración de Personal. La primera puede conocer de los documentos como currículo vitae, exámenes de control de confianza, referencias laborales, nombres de patrones previos, pero no conocerá del contrato que firme con la institución, su número de cuenta de depósito de nómina o los nombres de sus beneficiaros en sus seguros de vida, porque esto le corresponde por facultades a la Dirección de Administración de personal. No obstante, esta segunda Dirección sí conoce de todo lo que obtuvo la primera, porque son los insumos que integran el expediente personal del ahora servidor público.

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso o tratamiento, y las atribuciones o facultades normativas que resulten aplicables.

Generar un catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales

Esto se refiere a identificar cómo se obtienen los datos personales, por medio de formatos en papel, es decir en físico, o un formato en línea, esto es electrónica, o bien, puede ser que el titular lo lleve por su cuenta en escrito libre en físico, y posteriormente se digitalice.

Identificar los medios de obtención de los datos personales y base de legitimación conforme a la Ley para su tratamiento

En este paso, tiene relación con la anterior, y trata de identificar los medios de obtención de los datos personales, pues existen diversas maneras por las cuales se pueden obtener los datos personales, entre ellas encontramos las siguientes:

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
    - Vía telefónica
    - Por correo electrónico
    - Por Internet o sistema informático
    - Por escrito presentado directamente en las oficinas del sujeto obligado

    - Por escrito enviado por mensajería

- Mediante una transferencia
    - Quién transfiere los datos personales y para qué fines
    - Medios por los que se realiza la transferencia

  Particularmente para el caso en que los datos personales sean obtenidos de una transferencia, es necesario identificar al tercero que realizó la transferencia de los datos personales y las finalidades de la recepción de los datos personales a partir de esta.

- De una fuente de acceso público

Es decir, de aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la Ley General y demás normativa aplicable.

Identificar los datos personales que se están tratando y su ubicación

En este paso deben señalar puntualmente mediante una descripción por tipo de dato o por categoría de datos personales cuáles son los datos que tiene en su posesión, adicionalmente añadir la ubicación física de los datos. Por lo que puede contestar las siguientes preguntas:

- ¿Qué tipo de datos personales se tratan? ¿son sensibles?

Si en el concentrado de datos personales que se tiene, existen datos que, de acuerdo con la definición de la Ley General, sean datos sensibles, es decir, datos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se refieren a aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

- ¿Dónde se almacenan y realiza el tratamiento de los datos personales?

Se elaborará un catálogo de los tipos de datos personales que se tratan en donde además de identificar el tipo de dato personal que almacena, se indica al menos los siguientes elementos:

- Formato en que se encuentra la base de datos: primero debe tomar en cuenta el concepto de formato de apoyo, es decir, indicar el formato en el que se resguardan los datos personales, por ejemplo, un formulario impreso en hojas de papel en el que se registraron los datos, copias de identificaciones de los titulares de datos o bien formularios digitalizados,

es decir, indicar si la base de almacenamiento de datos se encuentra en formato físico y/o electrónico
- Ubicación de la base de datos: señalar una descripción general de la ubicación física de los activos de apoyo en los que se encuentran los datos personales
- Sección, serie y subserie de archivos: en materia de archivos puede incluir este tipo de información para un mejor manejo de dichos activos.

Identificar las finalidades por las que se tratan los datos personales

Se deberán describir las causar por las que se tratan los datos personales dentro de los procesos internos de la unidad administrativa, por ejemplo, el procedimiento podría ser "contratación de personal" y las finalidades "evaluación de currículum para la selección de personal".

Además, es necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos de excepción al consentimiento (fracciones) del artículo 22 de la Ley General actualizan.

Identificar quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado

Se debe identificar el catálogo de servidores públicos al interior del sujeto obligado que tienen acceso a los datos personales y para qué fin, señalando los siguientes puntos:

- Un listado de los puestos de los servidores públicos que intervienen en alguna actividad derivada del tratamiento realizado identificando su área de adscripción;
- Las finalidades por las cuales el servidor público identificado tiene acceso a los datos, y
- Los privilegios que tiene cada usuario sobre el tratamiento y sobre los activos involucrados en el tratamiento, por ejemplo, si tiene acceso para consultar, modificar, generar copias, eliminar o actualizar cualquier dato identificado como parte del sistema de tratamiento.

Identificar si intervienen encargados en el tratamiento de los datos personales

Es necesario determinar si se existen encargados de tratamiento de datos personales, recordando que son aquellas personas físicas o jurídicas, públicas o privadas, **ajena a la organización del responsable**, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

De ser así, se debe integrar el nombre del encargado y el número o nomenclatura con la que se identifique el instrumento jurídico que consolide la relación entre responsable y encargado.

Identificar si se realizan transferencias de los datos personales recabados

Las transferencias son toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, por lo que, tiene que reconocer si realiza alguna comunicación conforme a la descripción.

En este paso se señala qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad.
Si se encuentra en este supuesto, será necesario precisar:

- Las autoridades o terceros externos a la institución a quienes se comunican los datos personales
- Las finalidades que justifican las transferencias.
- Señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos de excepción (fracciones) de los artículos 22, 66 o 70 de la Ley General actualizan.

Identificar si se difunden los datos personales

En este paso se identifica si en el tratamiento declarado se realiza una difusión de datos personales, en este caso, se tiene que indicar el fundamento jurídico que autoriza la difusión.

Mencionar el plazo de conservación de los datos personales

Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

Una vez que se haya realizado un diagnóstico en materia archivística, estará preparado para cumplir de mejor manera con las obligaciones previstas en la Ley General y los Lineamientos Generales.

Identificar el plazo de bloqueo de los datos personales previo a la eliminación de estos

El bloqueo se refiere a la identificación y limitación del tratamiento de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estos. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido este, se procederá a su cancelación en la base de datos que corresponda.

El inventario de datos personales y sistemas del tratamiento deberá mantenerse actualizado a lo largo del tiempo ya que es indispensable saber los activos con los que cuenta el sujeto obligado para poder protegerlos correctamente, ya que

como se verá adelante, el inventario es la base para elaborar el análisis de riesgos y el análisis de brecha.

Finalmente, es preciso señalar que el INAI ha creado una propuesta de inventario, incluido en los anexos del Programa de Protección de Datos Personales y cuenta los elementos enlistados y puede ser consultado en la página web, se trata del **ANEXO A. Formato de Inventario de datos personales y sistemas de tratamiento**[31] de dicho- documento.

Paso 4. Establecer funciones, obligaciones, roles y privilegios de quienes tratan datos personales, así como la cadena de rendición de cuentas

Una vez que tenemos identificados los tratamientos de datos personales al interior del sujeto obligado a través del inventario de datos personales y sistemas de tratamiento, así como los propios datos personales (activos de información) y los activos de apoyo, podremos identificar también quienes son las personas que realizan los tratamientos de datos personales a diario, y por lo tanto se podrán fijar y documentar sus funciones, obligaciones, roles, responsabilidades, así como la rendición de cuentas respecto del activo identificado.

Para efectos del sistema de gestión se debe identificar qué persona tiene la responsabilidad del tratamiento de los datos personales y por lo tanto del o los activos que contienen, almacenan, procesan, transmiten y/o eliminan los datos personales, puede ser, por ejemplo, un sistema electrónico y bases de datos electrónicas o físicas, es decir, el propietario del tratamiento y que puede ser quien esté a cargo de su producción, desarrollo, mantenimiento, uso y/o seguridad, según corresponda. Asimismo, deberá identificarse el o los custodios del tratamiento y por lo tanto del o los activos que contienen, almacenan, procesan, transmiten y/o eliminan los datos personales, que serán aquellas personas con responsabilidad funcional sobre los activos, por ejemplo, los administradores de esas bases de datos. Para efectos del análisis del riesgo, particularmente en la valoración de los activos, el propietario y los custodios del activo pueden ser las personas idóneas para determinar el valor que el activo tiene para la organización.

Respecto a este punto, al igual que el anterior, en caso de que el sujeto obligado haya elaborado previamente el Documento de Seguridad, podrá utilizar el documento a que refiere la fracción II del artículo 33, y fracción II del artículo 35, relativo a las funciones y obligaciones de las personas que traten datos personales, en caso contrario deberá de acuerdo con la Ley General y a los Lineamientos Generales, observar lo siguiente:

31 https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/AnexosDocumentoOrientador.zip

Artículo 33 de la Ley General:
"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. (...)

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;"

Artículo 57 de los Lineamientos Generales:

"Funciones y obligaciones
Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento."

En ese sentido, será importante que el responsable del tratamiento:

1. **Identifique al personal que realiza el tratamiento de datos en cualquiera de las fases o durante el ciclo de vida del dato.**

Para ello es posible apoyarse del inventario de datos personales y sistemas de tratamiento, en tanto que en este se encontrarán mapeados los flujos de los datos personales, por tratamiento dentro de la entidad, a fin de reconocer las unidades administrativas que interactúan en el tratamiento, y los servidores públicos que participan.

2. **Designe funciones y obligaciones.**

Una vez se ha identificado la participación del personal en el tratamiento o la fase correspondiente, se deben definir y documentar sus funciones y obligaciones y los roles y responsabilidades, así como establecer lo que puede y debe hacer, y lo que no, con los datos personales y los activos de apoyo. Es así que resulta indispensable que en la documentación de las funciones y obligaciones del personal que trata datos personales se justifique el tratamiento a través de sus facultades conforme a la normativa aplicable al sujeto obligado (Leyes, Reglamentos, manuales de procedimiento, manual de organización, etcétera).

Funciones y obligaciones deberá entenderse como todo aquello que está permi-

tido o prohibido realizar en materia de protección de datos personales, tanto de manera general para todos los involucrados en el tratamiento de datos personales, como de forma particular para ciertos roles.

Respecto a la asignación de los roles, estos deben estar claros y bien definidos, de manera general podemos enlistar algunos roles como lo son:

- Propietario
- Custodio
- Administrador
- Usuario

Estos roles se encuentran definidos por las actividades que los involucrados en el tratamiento de datos personales realizan con los activos de apoyo o activos donde se procesan y/o resguardan los datos personales, como lo pueden ser bases de datos electrónicas o físicas, sistemas electrónicos, servidores, entre otros. Es así que, a partir de esta relación, se pueden comenzar a definir los privilegios que tendrá cada uno, esto quiere decir que se deben restringir las actuaciones que puede realizar cada perfil en ese activo.

Por ejemplo, no debe ser el mismo privilegio otorgado a los custodios que administran una base de datos electrónica, que la que tenga un usuario donde su función solo sea visualizar los datos personales, el privilegio de este último debe estar restringido a solo visualización, sin permitírsele, modificación, copia o borrado.

Adicionalmente, en el espectro de la seguridad de la información, es posible describir los roles como funciones específicas que conllevan responsabilidades en materia de seguridad de la información, por ejemplo:

- CISO, (Chief Information Security Officer) que podría traducirse como Director u Oficial de Seguridad de la Información.[32]
- CSOs (Chief Security Officer) responsable de seguridad de la organización, o de seguridad corporativa, en organizaciones pequeñas es frecuente que coincidan ambas responsabilidades en una misma persona.[33]
- CIO (Chief Technology Officer) puede decirse que es el responsable de innovación en tecnologías en la entidad.[34]
- CTO (Chief Information Officer) Responsable o Director de Tecnologías de la información.[35]

Para el sector público, es posible identificar un rol establecido en la Ley General, que es el Oficial de Protección de Datos Personales, quien tendrá la responsabilidad de realizar las funciones establecidas en el artículo 89 de la Ley General[36]

32 INCIBE Blog, Roles en ciberseguridad: desde el CEO a los usuarios finales, 20 de junio de 2023, disponible en: https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales Fecha de consulta: 26-09-2023.

33 Idem

34 Idem

35 Idem

36 Artículo 85. Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará

(las atribuciones de la Unidad de Transparencia, enfocadas a protección de datos personales).

Si bien, estos roles no son obligatorios por Ley, es recomendable a manera de buena práctica, aunque no se realicen tratamientos intensivos de datos personales, establecer alguno de estos roles, que se encargue por lo menos de la gestión de la seguridad de la información, así como de gestionar los incidentes de seguridad de la información y protección de datos personales.

3. Establecer la cadena de rendición de cuentas

La definición de roles dará como consecuencia lógica la cadena de rendición de cuentas, puesto que identificar quien será el propietario del activo o sistema que contiene los datos personales, dentro del tratamiento o de la fase del tratamiento correspondiente, y quien será el custodio del tratamiento, es decir, quien tenga la responsabilidad operativa del o los activos, a efectos de asignar las responsabilidades correspondientes derivado, por ejemplo, de un mal tratamiento de datos personales, y quien o quienes son los usuarios de los activos, brinda la trazabilidad de la operación y el tratamiento de los datos personales, por lo que si se diera alguna vulneración de los datos personales, podría darse fácilmente con la persona responsable, en caso de tener bien documentada la política correspondiente y configurados con las restricciones conducentes los perfiles y privilegios.

Cabe destacar que este paso de definir funciones y obligaciones, roles y responsabilidades, perfiles y privilegios debe quedar asentado en una política de gestión y tratamiento de datos personales, y esta debe ser comunicada al personal involucrado en el tratamiento, y de ser el caso, brindar la sensibilización o capacitación correspondiente, ya que una política no funciona como medida de seguridad, sin estos pasos posteriores (la comunicación a los involucrados, y la capacitación). Finalmente debe decirse que los perfiles y privilegios deberán quedar asentados y revisarse periódicamente para el caso de altas y bajas de personas trabajadoras.

Derivado del establecimiento de las funciones y responsabilidades como de los

---

conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia. (...)

perfiles y privilegios, se podrá proyectar el tipo de capacitación que requerirá el personal, ya que no será el mismo nivel de capacitación que requiera una persona que realiza el tratamiento de datos personales en papel, o que simplemente accede a revisar datos en una base de datos, sin tener que manipularla, a un administrador de la propia base de datos.

4. **Comunicar las funciones y responsabilidades a los interesados.**

Como se mencionó, una vez definidas las funciones y obligaciones, roles y responsabilidades, el responsable deberá asegurarse de que todos los involucrados conozcan sus propias atribuciones, funciones y obligaciones en el tratamiento de los datos, así como las consecuencias en el caso de incumplimiento.

Es recomendable que la documentación de roles y responsabilidades esté armonizada con el análisis de brecha y el plan de trabajo donde se establezca qué servidor público será el propietario y custodio del tratamiento o del activo en particular, así como el propietario o responsable de operar la implementación de medidas de seguridad del activo o tratamiento correspondiente.

Paso 5. Gestión de riesgos: valorar y tratar el riesgo de los datos personales, los activos que los contienen y sistemas de tratamiento

La Ley General en su artículo 33, fracción IV indica que debemos establecer las medidas de seguridad mediante un enfoque de análisis del riesgo. Debemos comprender que a nivel de metodologías y estándares internacionales el análisis de riesgo es una parte del proceso de la gestión del riesgo, que la Ley General no señala expresamente; sin embargo, para efectos de un correcto cumplimiento del deber de seguridad y particularmente para el cumplimiento del artículo 34 de la Ley General que mandata la implementación de un sistema de gestión, lo correcto es implementarlo conforme al enfoque de la gestión del riesgo, lo que comprende también el análisis.

En ese sentido el sistema de gestión debe estar basado en la comprensión de la naturaleza del riesgo al que están expuestos los datos personales y los sistemas del tratamiento para así mantenerlo en niveles adecuados, en el entendimiento de que el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la implementación de medidas de seguridad y a través de la mejora continua del sistema de gestión.

El objetivo de esta sección es que los responsables valoren el riesgo, identificando sus características que mayor impacto pueden tener sobre los datos personales que tratan o bien, en los sistemas de tratamiento, o los activos que soporten los tratamientos, y posteriormente, se valore la probabilidad de ocurrencia de los riesgos y el impacto que puede llegar a causar a los titulares, en escalas cuantitativas y cualitativas, para evaluarlos comparando los resultados con los criterios establecidos en el Paso 1.2. (Definición de la metodología

y criterios mínimos de la gestión de riesgos); y finalmente tratarlos, priorizando los riesgos más relevantes a tratar y seleccionando las medidas necesarias para mantenerlo en niveles aceptables.

5.1. Valoración del riesgo

La valoración del riesgo comprende a su vez la identificación, el análisis y la evaluación. Para la identificación de los riesgos debe considerarse previamente la elaboración de un inventario de activos, el cual comprende a su vez la identificación de activos para posteriormente evaluar su criticidad o grado de importancia para la protección de los datos personales.

Identificación de activos-inventario de activos

En este paso deben identificarse los activos de información y de apoyo[37].

Si bien en el Paso 3 ya se desarrolló el inventario de datos personales y sistemas de tratamiento, para este momento es necesario revisar como tal los activos sobre todo de apoyo, es decir esos activos en los que los datos personales se almacenan, procesan o transmiten, por ejemplo: las computadoras, bases de datos, servidores, archiveros, entre otros, ya que estos son los que se van a someter a la gestión del riesgo.

En ese sentido, es posible utilizar como base (y será de mucha ayuda) el inventario de datos personales y sistemas de tratamiento.

En este paso puede utilizar el inventario de datos personales y sistemas de tratamiento a que refiere el Paso 3 (Identificación de tratamientos de datos personales activos que los soportan y sistemas de tratamiento) y plasmarlo en un inventario de activos. Asimismo, se recomienda que para realizar la gestión de riesgos se considere aplicar los siguientes pasos a los sistemas de tratamiento, es decir, al conglomerado de datos definido por cada formato declarado como sistema, no así a los datos personales en lo particular, ya que la valoración del riesgo cambia de acuerdo al contexto en que se encuentre el dato personal, es decir el entorno (físico o electrónico), el activo de apoyo en el que se obtenga almacene o transmita. declarar.

37 En materia de protección de datos personales, y en armonía con la Guía de apoyo para la elaboración del Documento de Seguridad, los activos se dividen en dos tipos, activos de información que son propiamente los datos personales y los activos de apoyo, que son los elementos físicos e infraestructura que soportan los activos de información. INAI, Guía de apoyo para la elaboración del Documento de Seguridad Páginas 34 y 44. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf consultada el 02/04/2024.

Valoración de activos

Una vez identificados los activos, se deben valorar a efectos de comprender su criticidad e importancia para el sujeto obligado pero enfocado en la protección de los datos personales, por ejemplo, un activo será más relevante si, contiene datos personales y se utiliza en algún tratamiento sustantivo del sujeto obligado, es decir, que sea un proceso sustancial para cumplir los objetivos por los que fue creado o existe el sujeto obligado, o si bien, siendo un tratamiento adjetivo, el activo contiene o procesa datos personales, datos personales sensibles o una gran cantidad; una vez determinado lo anterior, la forma de valorarlos debe ser conforme a los criterios establecidos en el Paso 1.2. (Definición de la metodología y criterios mínimos de la gestión de riesgos) por cada propiedad de la información.

Si en el establecimiento de criterios para la valoración de activos se estableció que se valorará cada uno de los activos en las tres propiedades en una escala de valor de 1 a 3, donde 1 es bajo o poco crítico, 2 es medio y 3 alto o crítico, entonces se realizará lo siguiente:

a) Determinar el valor del activo en función de los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, aplicándose la escala referida con antelación, esta valoración resulta necesaria para conocer el riesgo inherente de cada activo que conforma el sistema de tratamiento.

Valor Cualitativo	Valor Cuantitativo
Bajo	1
Medio	2
Alto	3

Tabla 4. Ejemplo de escala para valorar las propiedades de la información: confidencialidad, integridad y disponibilidad, para la valoración de activos.
Autoría propia

b) Calcular el valor del activo, por ejemplo, sumando los valores asignados a cada propiedad de la información (confidencialidad, integridad y disponibilidad), empleándose la siguiente escala para obtener el valor (cualitativo y/o cuantitativo) final, deberá considerarse que, si el tratamiento, activo o sistema de tratamiento incluye o almacena datos sensibles, estos deberán ser considerados con el valor más alto por su naturaleza.

Valor Cualitativo	Valor Cuantitativo
Bajo	1 - 3
Medio	4 - 6
Alto	7 - 9

Tabla 5. Ejemplo de escalas cuantitativas y cualitativas, resultado de la suma de los tres valores asignados a las tres propiedades de la información
Autoría propia

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se pueden realizar las siguientes preguntas:

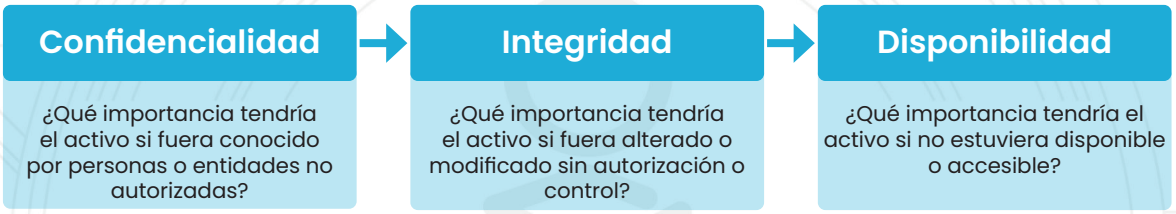


Figura 7. Preguntas para valorar la Confidencialidad, integridad y disponibilidad de los datos personales contenidos en los activos de apoyo.
Autoría propia

Ya que se ha establecido el valor por cada propiedad de la seguridad de los datos, debe obtenerse un valor único, por ejemplo, sumando los tres valores y estableciendo el valor cualitativo único de acuerdo con la tabla denominada "Ejemplo de escalas cuantitativas y cualitativas".

Ejemplo práctico:

Supongamos que pertenecemos al sujeto obligado Ministerio de Educación que tiene a su cargo el Registro de todos los estudiantes de todos los niveles del país. Nuestra unidad administrativa es propietaria del tratamiento de datos personales correspondiente al Registro de Estudiantes de Nivel Medio Superior (RENMS). Respecto a dicho tratamiento, la unidad administrativa ha identificado los siguientes activos en los que se resguardan datos personales de los estudiantes de nivel medio superior del país:

- Un Sistema Automatizado para el control del Registro de Estudiantes de Nivel Medio Superior (RENMS) que cuenta con un servidor de base de datos propio del Ministerio (Servidor 1) en el que se almacenan, gestionan y administran datos pertenecientes a los diversos sistemas informáticos de las unidades administrativas que integran el Ministerio.
- Una base de datos compuesta por documentos físicos de estudiantes de Nivel Medio Superior, la cual contiene solo una parte de lo que se almace-

na y procesa en la base de datos electrónica, ya que desde hace 3 años se migró por completo al sistema electrónico, y

- 45 equipos de cómputo asignados a los servidores públicos de la unidad administrativa, quienes tienen atribuciones para tratar datos personales de las personas estudiantes, toda vez que pueden descargar la base de datos electrónica del Sistema Automatizado de Registro de estudiantes de Nivel Medio Superior.

Se identificó durante la elaboración del inventario de datos personales y sistemas de tratamiento y posteriormente en el inventario de activos que, los datos personales tratados en esos activos son:

Activo de apoyo	Datos Personales que contiene, almacena, procesa o transmite.
Sistema automatizado de registro ENMS (RENMS)	**De los estudiantes:** Nombre(s) y apellidos Nacionalidad Fecha de nacimiento Edad Población de nacimiento Dirección Particular Teléfono fijo Teléfono de emergencia Correo electrónico Historia académica: escuelas en las que ha estado inscrito la persona estudiante Calificaciones En algunos casos, diagnósticos de enfermedades y de discapacidades. Nombre(s) y apellidos de madre, padre o tutor.
Base de datos física	**De los estudiantes:** Nombres y apellidos de estudiantes Nacionalidad Fecha de nacimiento Edad Población de nacimiento Dirección Particular Teléfono fijo Teléfono de emergencia Correo electrónico Historia académica: escuelas en las que ha estado inscrito la persona estudiante Calificaciones En algunos casos, diagnósticos de enfermedades y de discapacidades. Nombres y apellidos de madre, padre o tutor.

Computadoras de personas servidoras públicas de la UA.	**De los estudiantes:** Nombres y apellidos de estudiantes Nacionalidad Fecha de nacimiento Edad Población de nacimiento Dirección Particular Teléfono fijo Teléfono de emergencia Correo electrónico Historia académica: escuelas en las que ha estado inscrito la persona estudiante Calificaciones En algunos casos, diagnósticos de enfermedades y de discapacidades. Nombres y apellidos de madre, padre o tutor. **Datos personales propios del servidor público:** diversos datos.

Tabla 6. Listado de activos de apoyo con los datos personales que almacenan o procesan (ejemplo)

Ahora, sabiendo la naturaleza de los datos personales que estos activos contienen, procesan, almacenan o transmiten, se deben valorar con un enfoque de la importancia en lo general que tienen para el sujeto obligado y de acuerdo con la naturaleza los datos personales la importancia que tendrían para las personas titulares de eso datos personales.

La propuesta es la siguiente, de acuerdo con las preguntas establecidas en la figura 7. Para este ejemplo, se analizará solo un activo, el RENMS:

- Para la confidencialidad: ¿Qué pasaría si terceros no autorizados acceden al RENMS, y por lo tanto a la información que en él se contiene y procesa? ¿o si siendo autorizados para su tratamiento divulgan información? ¿Tendría relevancia para el sujeto obligado, sus procesos y para las personas titulares?
- Para la integridad: ¿Qué pasaría si personas no autorizadas modifican, manipulan o alteran la información que almacena, procesa o transmite el RENMS? ¿Tendría relevancia para el sujeto obligado, sus procesos y para las personas titulares?
- Para la disponibilidad: ¿Qué pasaría si personas no autorizadas impiden la operatividad del RENMS y por esa circunstancia las personas autorizadas para su tratamiento no pueden acceder a la información que en el se contiene, procesa o transmite? ¿Tendría relevancia para el sujeto obligado, sus procesos y para las personas titulares?

Análisis de los tres activos del caso:

Activo	Valor del activo por dimensión			Valor total cuantitativo	Valor total cualitativo
	Confidencialidad	Integridad	Disponibilidad		
1. Sistema electrónico RENMS-BBDD	**3** La pérdida de confidencialidad de la información del sistema electrónico puede ser muy grave en tanto que contiene datos personales de menores de edad y en algunos casos datos sensibles de personas menores de edad, en ese sentido puede traer consecuencias graves para las personas y consecuencias legales para el sujeto obligado.	**3** La modificación no autorizada o pérdida de parte de la información puede traer consecuencias en los procesos internos del sujeto obligado, ya que trae consecuencias legales para éste y consecuencias para las personas titulares.	**3** El no tener disponible esta base de datos o el sistema, puede causar retrasos en los procesos críticos que son objetivos fundamentales del sujeto obligado.	**9**	**Alto**
2. Base de datos física del Registro de ENMS	**3** La pérdida de confidencialidad de la información de la base de datos física puede ser grave en tanto que contiene datos personales de menores de edad y en algunos casos datos sensibles de personas menores de edad, en ese sentido puede traer consecuencias legales para el sujeto obligado.	**3** La modificación no autorizada o pérdida de parte de la información puede traer consecuencias en los procesos internos del sujeto obligado y consecuencias para las personas titulares.	**1** La pérdida de disponibilidad de este activo no representa gravedad para seguir operando el proceso, toda vez que esta base de datos es de archivo, está incompleta y actualmente se utiliza el Sistema Electrónico.	**7**	**Alto**

3. 45 computadoras de personas servidoras públicas de la UA	**3** La pérdida de confidencialidad de la información del sistema electrónico puede ser muy grave en tanto que contiene datos personales de menores de edad y en algunos casos datos sensibles de personas menores de edad, y puede contener información personal, incluso sensible, de la persona servidora pública.	**3** La modificación no autorizada o pérdida de parte de la información puede traer consecuencias en los procesos internos del sujeto obligado y consecuencias para las personas titulares.	**1** La pérdida de disponibilidad de uno o más de estos activos puede atrasar los tiempos de procesamiento de la información, pero no representa un conflicto grave, en tanto que se tienen más computadoras donde se puede descargar la información y continuar con los trabajos.	**7**	**Alto**

Tabla 7. Ejemplo de valoración de los activos
Autoría propia

Respecto al ejemplo anterior, no es necesario justificar en una tabla los valores cuantitativos, sin embargo, sí debe estimarse con razonamientos lógicos, por lo que se ha puesto la justificación del valor a modo de ejemplo.

Nótese que para la valoración debe justificarse la importancia de cada propiedad de la información para el propio activo, para el sujeto obligado y el cumplimiento de sus objetivos y como estos pueden incidir en la protección de datos personales, si bien desde este momento se puede observar el impacto en las personas titulares o las consecuencias, en este paso no es determinante, puesto que el análisis del impacto se hace posteriormente; el enfoque cambia ya que puede ser, por ejemplo, que en la valoración del activo en disponibilidad sea indispensable, pero en el impacto para las personas titulares, sea despreciable, o muy bajo.

Para concluir este apartado, es relevante señalar que por cada activo se deberá identificar un propietario, es decir, una persona o unidad administrativa (área que trata los datos personales) con la responsabilidad y la autoridad para gestionar un activo (por ejemplo, el titular del área). Es recomendable que el propietario del activo junto con el custodio, determinen el valor de este, puesto que son quienes conocen la operación del tratamiento de datos y la incidencia del activo en el propio tratamiento.

Identificación de 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 del sujeto obligado. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Los propietarios, custodios y usuarios de los activos 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 área 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.

Las amenazas son acciones que ocurren y que pueden causarles daño a nuestros activos, son muy variadas y van cambiando con el tiempo. El desarrollo tecnológico, las comunicaciones y la información van asociadas, al tiempo van unidas al surgimiento de nuevas formas de vulneración de los datos personales, al honor, la intimidad personal y familiar e incluso a la propia imagen.

Por ello, es importante mencionar que, no todas las amenazas afectan a todos los activos, sino que hay cierta relación entre el tipo de activo y lo que le podría ocurrir.

En este paso se recomienda realizar las siguientes actividades:

a) Identificar todas las amenazas relacionadas con cada activo. Las amenazas se pueden identificar utilizando los catálogos definidos para tal fin en las metodologías de gestión de riesgos.

b) Se debe tomar en cuenta que cada activo puede estar relacionado con múltiples amenazas, y cada amenaza puede estar vinculada con varias vulnerabilidades.

c) La identificación de amenazas será realizada con la ayuda de los propietarios y custodios de los activos.

Las amenazas de acuerdo con las diversas metodologías de gestión de riesgos explicadas en este documento se pueden dividir en diversos grupos, se ejemplifican tres grandes grupos con algunos ejemplos de los tipos de amenazas, los cuales son:

- Deliberadas. Son aquellas causadas por las personas que acceden a los sistemas de información, quienes pueden causar problemas intencionados, ya sea con el ánimo de beneficiarse indebidamente, o bien, con la intención de causar daños y perjuicios a los activos, a la organización, y por lo tanto a las personas titulares de los datos personales[38].
- Ambientales. Aquellas que devienen de fenómenos naturales como terre-

38 Definición basada en Rodríguez José María y Peralta Ignacio. 2013. Administración electrónica, Gestión de riesgos, Magerit. tiThink, p.13

motos e inundaciones[39].

- Accidentales. Son aquellas causadas por las personas con acceso al sistema de información quienes pueden generar problemas no intencionados, típicamente por error o por omisión[40].

Tipo	Amenaza	Origen
Daño físico	Fuego accidental	Deliberada, Ambiental
	Daños por agua	Accidental, Deliberada, Ambiental
	Contaminación accidental	Deliberada, Ambiental
	Accidente grave	Accidental, Deliberada, Ambiental
	Destrucción de equipos o medios	Accidental, Deliberada, Ambiental
	Polvo, corrosión, congelación	Accidental, Deliberada, Ambiental
Eventos naturales	Fenómeno climático	Ambiental
	Fenómeno sísmico	Ambiental
	Fenómeno volcánico	Ambiental
	Fenómeno meteorológico	Ambiental
	Inundación por fuerza natural	Ambiental
Pérdida de servicios esenciales	Fallo del sistema de suministro de agua o aire acondicionado	Deliberada, Ambiental
	Pérdida de suministro de energía	Accidental, Deliberada, Ambiental
	Fallo del equipo de telecomunicaciones	Deliberada, Ambiental
Perturbación debido a radiación	Radiación electromagnética	Accidental, Deliberada, Ambiental
	Radiación termal	Accidental, Deliberada, Ambiental
	Pulsos electromagnéticos	Accidental, Deliberada, Ambiental

39 Ídem
40 Ídem

Información comprometida	Intercepción de señales de interferencia comprometedoras	Deliberada
	Espionaje remoto	Deliberada
	Escuchar deliberadamente a escondidas	Deliberada
	Robo de soportes o documentos	Deliberada
	Robo de equipo	Deliberada
	Recuperación de medios reciclados o desechados	Deliberada
	Divulgación	Deliberada
	Datos de fuentes no confiables	Deliberada, Ambiental
	Manipulación de hardware	Deliberada
	Manipulación de software	Deliberada, Ambiental
	Detección de posición	Deliberada
Fallas técnicas	Falla en el equipo	Ambiental
	Mal funcionamiento del equipo	Ambiental
	Saturación del sistema de información	Deliberada, Ambiental
	Mal funcionamiento del software	Ambiental
	Incumplimiento del mantenimiento del sistema de información	Deliberada, Ambiental
Acciones no autorizadas	Uso no autorizado de equipos	Deliberada
	Copia fraudulenta de software	Deliberada
	Uso de software falsificado o copiado	Deliberada, Ambiental
	Corrupción de datos	Deliberada
	Tratamiento ilegal de datos	Deliberada

Compromiso de funciones	Error en uso	Ambiental
	Abuso de derechos	Deliberada, Ambiental
	Forja de derechos	Deliberada
	Negación de acciones	Deliberada
	Incumplimiento de disponibilidad de personal	Accidental, Deliberada, Ambiental

Tabla 8. Ejemplos de amenazas y su clasificación

Ejemplo práctico de identificación de amenazas:

Continuando con el ejemplo previo, identificando al activo que se va a analizar es el Sistema electrónico RENMS-BBDD.

Ahora bien, supongamos que el contexto del sujeto obligado es el siguiente:

El Sistema electrónico RENMS-BBDD está alojado en el servidor del Ministerio. De la realización de una inspección al espacio físico donde se encuentra dicho servidor, se aprecian de manera casi imperceptible la presencia de manchas de humedad en las paredes, las cuales coinciden con la ubicación de tuberías de agua de la instalación, destacando que el edificio sede y su infraestructura tienen 52 años de antigüedad y nunca se habían presentado rastros de humedad en el edificio del Ministerio. Adicionalmente, se observa la falta de un servicio que brinde continuidad de suministro eléctrico, por lo que, en las últimas cinco ocasiones en las que se ha interrumpido el servicio, los sistemas informáticos dejan de estar disponibles por el tiempo de interrupción que no ha rebasado los 10 minutos.

Recientemente, la Dirección de Tecnologías de Información ha entregado un reporte del aplicativo correspondiente al Sistema electrónico RENMS-BBDD, en dicho reporte resaltan los siguientes hallazgos que tienen que ser revisados y en su caso atendidos lo más pronto posible:

- El sistema informático no tiene implementado un protocolo de intercambio seguro de información.
- No se identifica un control de descargas para los usuarios que tienen acceso a la BBDD.
- No se configuró un protocolo que soporte y administre una cantidad alta de demanda de servicio a fin de evitar la saturación del sistema, y no se cuenta con un servidor ni servicio que brinde redundancia[41].

41 De acuerdo con el Glosario de términos de ciberseguridad de INCIBE, la redundancia es la propiedad consistente en un determinado fichero o sistema para que en caso de caída de uno se pueda seguir proporcionando el servicio. (INCIBE, Glosario de términos de ciberseguridad, una aproximación para el empresario, España 2020, disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf).

- No se configuró un protocolo que identifique solicitudes maliciosas al sistema.

De acuerdo con el supuesto tenemos las siguientes amenazas:

Tipo	Amenazas
Sistema electrónico RENMS-BBDD	Pérdida de suministro de energía (Accidental)
	Daños por agua (Accidental, Deliberado o Ambiental)
	Divulgación de información (Deliberada)
	Robo de información (Deliberado)
	Saturación del sistema de información (Accidental)
	Negación de acciones (Deliberada)

Tabla 9. Identificación de amenazas del RENMS

Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Identificación de los eventos de vulneración, esto es identificar conforme a lo anterior los eventos donde es posible que una amenaza explote una vulnerabilidad y cause o pueda causar un daño en los activos, la organización y por lo tanto en los titulares de los datos personales.

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 redundancia consiste entonces, en tener el activo duplicado en más de un servidor y el balanceado de carga permite que se asigne a un servidor u otro en función de la carga de trabajo que esté soportando, en ese sentido si por cualquier situación un activo pierde disponibilidad el otro puede seguir operando y no se pierde la continuidad del servicio.

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.

Ejemplo:

Tipo	Amenaza	Origen
Sistema electrónico RENMS-BBDD	Pérdida de suministro de energía (Accidental)	No se cuenta con un sistema de respaldo de servicio eléctrico que brinde continuidad al servicio en caso de interrupción de suministro eléctrico.
	Daños por agua (Accidental, Deliberado o Ambiental)	El servidor de la institución se encuentra cerca del paso de tuberías de agua que llevan operando por más de 50 años.
	Divulgación de información (Deliberada)	Falta de administración de perfiles de acceso a la BBDD
	Robo de información (Deliberado)	No se cuenta con protocolos de intercambio seguro de información
	Saturación del sistema de información (Accidental)	Falta de configuración de sobre carga de paquetes
	Negación de acciones (Deliberada)	Falta de configuración filtrado de tráfico para identificar solicitudes maliciosas

Tabla 10. Identificación de vulnerabilidades del RENMS

Es así como la tabla sirve de ejemplo para que a partir de las amenazas identificadas en el paso anterior pueda asociar algunas vulnerabilidades, ya que, cada amenaza requiere de una o varias vulnerabilidades que pueda explotarla.

Es importante señalar que estas vulnerabilidades se aprecian ante un contexto de falta de medidas de seguridad, sin embargo, para la obtención del riesgo inherente como se observará adelante, se requiere justamente analizar las vulnerabilidades más propensas o posibles ante un supuesto donde no hubiese ninguna medida de seguridad.

Identificación de escenarios de vulneración

Una vez identificados los activos, sus vulnerabilidades y las amenazas, entonces se deben crear los escenarios donde el riesgo se materializa, es decir, donde la amenaza explota la vulnerabilidad, lo que inevitablemente trae una consecuencia para el activo, la entidad y los titulares de los datos personales.

Ejemplo de escenarios de vulneración

Activo	Valor total del activo	Amenaza	Vulnerabilidad	Escenario de vulneración
Sistema electrónico RENMS-BBDD	9-Alto	Pérdida de suministro de energía (Accidental) (si bien no es una amenaza directa, impacta directamente a todos los sistemas, aplicaciones, soportes, servidores del sujeto obligado)[41]	No se cuenta con un sistema de respaldo de servicio eléctrico que brinde continuidad al servicio en caso de interrupción de suministro eléctrico.	Interrupción de servicio del aplicativo por indisponibilidad por falta de suministro eléctrico.
		Daños por agua (Accidental, Deliberado o Ambiental)	El servidor de la institución se encuentra cerca del paso de tuberías de agua que llevan operando por más de 50 años. Si bien el activo que se está analizando es el RENMS, este se aloja en un servidor propio del Ministerio, de acuerdo al ejemplo, por lo que si se realiza un árbol de dependencias de activos, las amenazas que afecten al servidor de la Institución, afectarán a los activos que de él dependen.[42]	Perdida de información del RENMS por destrucción total o parcial del servidor en el que se aloja.

42 Para comprender como es que ciertas amenazas que se dirijan a ciertos activos pueden afectar a otros, es recomendable en la elaboración del inventario de activos realizar un mapeo y un árbol de dependencias de activos (que pueden ser la información misma, los servicios que se prestan, las aplicaciones software, el hardware hasta llegar a las instalaciones físicas) donde es posible observar que, si una amenaza afecta la seguridad de uno, va a afectar a todos los demás. Para mayor comprensión, se recomienda la lectura de la metodología MAGERIT 3.0, la cual explica de manera práctica el árbol de dependencias de activos (Libro I).

43 Se reitera la precisión anterior.

Activo	Valor total del activo	Amenaza	Vulnerabilidad	Escenario de vulneración
		Divulgación o robo de información (Deliberada).	Falta de administración de perfiles de acceso a la BBDD.	Robo de información en bases de datos por generar copias no autorizadas.
		Robo de información (Deliberado).	No se cuentan con protocolos de intercambio seguro de información.	Robo de información en bases de datos por acceso de terceros no autorizados internos o externos, por intercepción de la información no cifrada.
		Saturación del sistema de información (Accidental).	Falta de configuración de sobre carga de paquetes.	Interrupción de servicio del aplicativo por sobre carga de solicitudes de usuarios.
		Negación de acciones (Deliberada).	Falta de configuración filtrado de tráfico para identificar solicitudes maliciosas.	Interrupción de servicio del aplicativo por sobrecarga de solicitudes maliciosas.

Tabla 11. Ejemplos de escenarios de vulneración que afectan al RENMS como caso de ejemplo

Análisis de riesgos

Una vez identificados los escenarios de vulneración, debemos realizar el análisis de riesgos donde deberemos identificar las posibilidades o probabilidad de que el riesgo se materialice, así como el impacto que tendría en los activos, en la entidad y especialmente en los titulares de los datos personales.

El análisis de riesgos es clave para la gestión del riesgo ya que con este podemos evidenciar cuantitativa y cualitativamente el nivel de riesgo para evaluarlo y revisar, si, es acorde al criterio de nivel de riesgo aceptable establecido para la entidad y cómo tratarlo.

La fórmula para la valoración del riesgo es:

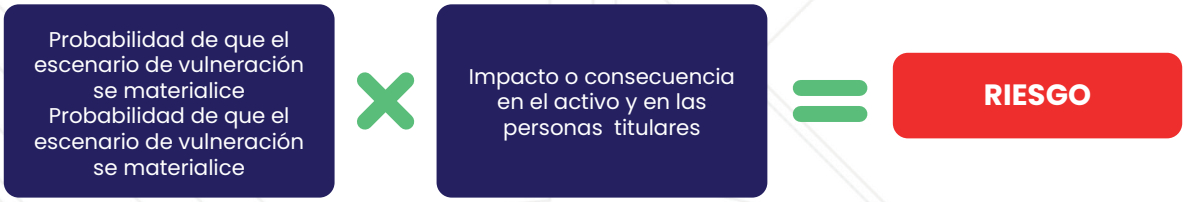


Figura 8. Fórmula para valorar el riesgo.
Autoría propia

¿Qué es un riesgo inherente?

La definición técnica del riesgo inherente es la valoración del grado de exposición de un activo a una amenaza que pueda explotar su vulnerabilidad, sin tener en cuenta ninguna medida de seguridad implementada.

En el caso que nos ocupa, es decir, tratándose de los datos personales como activo, adoptaremos como definición de riesgo inherente aquellos factores que le dan un valor significativo como para que cualquier persona no autorizada pudiera beneficiarse de ellos, y/o que por su naturaleza cause un mayor impacto en los titulares y/o en sus derechos y libertades.

Un ejemplo para mayor entendimiento es un dato personal sensible: este es un activo de información, su vulnerabilidad es ser sensible, por lo que, por su naturaleza, tendrá un nivel de riesgo inherente mayor, que un dato de identificación, en tanto que, de vulnerarse, pueden causar un mayor daño a las personas titulares.

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), o bien, cuando los datos que se tratan son sensibles[44].

Durante la implementación del sistema de gestión, la primera vez que realizamos el análisis de riesgos debemos obtener el riesgo inherente, donde debe calcularse la probabilidad de ocurrencia de la vulneración (el incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento) por el impacto en los activos de información que contienen datos personales y en los titulares ante la consolidación del escenario de vulneración que se esté analizando, todo esto sin considerar las medidas de seguridad ya implementadas, esto es así porque primero debemos tener un panorama claro de la criticidad intrínseca

44 Es importante recordar que el artículo 32 de la LGPDPPSO, precisa factores a considerar para el establecimiento de las medidas de seguridad con un enfoque en la gestión del riesgo de la seguridad de los datos personales, algunos de esos factores son: la sensibilidad de los datos, la tecnología utilizada, el número de personas titulares de quienes se tratan datos, las transferencias que se realicen, entre otros.

del propio activo y el escenario en el que se estaría de no contar con ninguna medida de seguridad; una vez se obtiene el riesgo inherente, y durante la primera parte para la elaboración del análisis de brecha, en el que ya se conocen las medidas de seguridad que ya están implementadas en el sujeto obligado, pero previo a decidir las medidas que faltan, se deberá valorar el riesgo residual, realizando una nueva iteración del análisis de riesgos, pero esta vez observando el nivel de degradación del riesgo al implementar la o las medidas de seguridad.

Así, sabremos si con las medidas actuales se mantiene el riesgo en un nivel aceptable o si es necesario implementar más medidas.

¿Cómo realizar el análisis de riesgos?

En este punto se deberá valorar el riesgo en escalas cuantitativas y/o cualitativas con los criterios establecidos en el paso 1.2. (Definición de la metodología y criterios mínimos de la gestión de riesgos) respecto a la probabilidad de que una vulneración se materialice, es decir, que una amenaza explote una vulnerabilidad; y respecto al impacto que tenga esta materialización en los activos y en los titulares de los datos.

De acuerdo con la Ley General el responsable para el análisis de riesgos debe considerar las amenazas, vulnerabilidades y los recursos involucrados en los tratamientos de datos personales, que en cuanto a metodología, ya se está cumpliendo puesto que se estaría considerado en la identificación de riesgos que es previo al análisis, asimismo conforme a los Lineamientos Generales, también debe considerar los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico, el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida, el valor y exposición de los activos involucrados en el tratamiento de datos personales y las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Artículo 33 de la Ley General:
"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, almenos, las siguientes actividades interrelacionadas:

II. (...)

III. (...)

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;"

Artículo 60 de los Lineamientos Generales:
"Análisis de riesgos
Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:
I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la Ley General."

Ejemplo de análisis de riesgos

Para este paso debemos considerar los criterios de probabilidad y de impacto fijados en el paso 1.2. (Definición de la metodología y criterios mínimos de la gestión de riesgos).

Probabilidad

Recordando lo señalado, la probabilidad es la posibilidad de ocurrencia de un hecho o acontecimiento, considerando la cantidad de veces que podría presentarse en determinado periodo de tiempo, basándose en las eventualidades conocidas y el conocimiento del entorno, o bien a través del juicio de una persona experta. En ese sentido deberá establecerse una escala cuantitativa y/o cualitativa considerando los escenarios previstos, y los registros, bitácoras, datos históricos con los que se cuente, o bien, auxiliándonos de expertos y el conocimiento del entorno.

Ejemplo de escala de probabilidad, suponiendo que nos basamos en registros de incidentes de seguridad del sujeto obligado y el análisis del entorno.

Grado de Probabilidad		Criterio
Muy baja	1	Si no se tiene registro de ningún tipo de antecedente registrado en los últimos 10 años y/o que por el entorno la posibilidad de que suceda sea mínima.
Baja	2	Si ha ocurrido un máximo de 3 antecedentes en un periodo de 5 años, o que por el entorno y condiciones sea poco probable que ocurra.
Media	3	Si se han registrado de uno a tres incidentes en un periodo anual y/o esporádicamente en intervalos de 3 a 5 años o que por el tipo de entorno y condiciones sea posible que ocurra en esos periodos.
Alta	4	Si se tiene registro de entre 3 y 5 eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea muy probable que suceda.
Muy Alta	5	Si han ocurrido más de cinco eventos en un periodo anual, y por las condiciones actuales o el tipo de entorno es inminente que ocurran constantemente.

Tabla 12. Criterios de probabilidad

Ejemplo de aplicación de la escala de probabilidad en el análisis de riesgos:

A partir del ejemplo de la Base de Datos electrónica-Registro de ENMS (BB-DD-RENMS), adicional a las amenazas físicas del inmueble (ver ejemplo práctico de identificación de amenazas) en el que se encuentra el servidor del Ministerio, se han identificado las siguientes anomalías generales y particulares:

- El RENMS no tiene implementado un protocolo de intercambio seguro de información.
- El RENMS no tiene configurados perfiles ni privilegios en la BBDD.
- En días recientes del lanzamiento del aplicativo se registró una falla en la operación del RENMS por la cantidad de usuarios que quisieron acceder al aplicativo y no se cuenta con un servidor que brinde redundancia.
- En días recientes, se ha registrado un tráfico inusual en la navegación de diversos servicios informáticos propiedad del Ministerio, al respecto, personal especializado intuye que puede tratarse de un ataque DDoS[45], que no se ha materializado y tampoco se identifica el servicio que tratan de atacar.

Evaluación de la probabilidad de ocurrencia					
Escenario de vulneración			**Probabilidad de ocurrencia**		**Justificación**
Amenaza	**Vulnerabilidad**	**Escenario de vulneración**	**Cuantitativa**	**Cualitativa**	**Descripción**
1. Pérdida de suministro de energía (Accidental)	No se cuenta con un sistema de respaldo de servicio eléctrico que brinde continuidad al servicio en caso de interrupción de suministro eléctrico.	Interrupción de servicio del aplicativo por indisponibilidad por falta de suministro eléctrico.	**3**	**Media**	Al año se registraron 2 interrupciones del servicio de suministro eléctrico, estos son esporádicos y pueden ser por periodos de tiempo no mayores a 10 minutos y no se tiene antecedente de humedad en el lugar.

45 Denegación de servicio es un ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. INCIBE, Glosario de Términos de ciberseguridad, fecha de consulta 12/07/2023. Disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf,

"Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática. Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red." INCIBE Blog. (21-08-2018). ¿Qué son los ataques DoS y DooS? Fecha de consulta 12/07/2023, disponible en https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos.

2. Daños por agua (Accidental, Deliberado o Ambiental)	El servidor de la institución se encuentra cerca del paso de tuberías de agua que llevan operando por más de 50 años.	Perdida de información por destrucción total o parcial del servidor.	3	Media	El promedio de vida útil de una tubería es de 50 años, en este año se observó que las paredes del lugar donde se encuentra el servidor (centro de datos) muestran de manera casi imperceptible rastros de humedad. [45]
3. Robo o Divulgación de información (Deliberada)	Falta de administración de perfiles de acceso a la BBDD.	Robo de información en bases de datos por generar copias no autorizadas.	5	Muy alto	No contar con gestión de perfiles y privilegios de la BBDD, no permite tener contabilidad y trazabilidad de las copias generadas. El contexto en este caso nos indica que el RENMS no tiene configurados perfiles ni privilegios, por lo que se puede intuir que es muy probable que varias personas cuenten con usuarios administradores, y los de perfiles de usuarios, no estén configurados, por lo que no tienen restricciones para descargar o modificar la base de datos. En ese sentido es muy probable que se materialice el escenario.
4. Robo de información (Deliberado)	No se cuentan con protocolos de intercambio seguro de información	Robo de información en bases de datos por acceso de terceros no autorizados internos o externos, por intercepción de la información no cifrada.	5	Muy alta	Al no estar implementados protocolos de intercambio seguro de información en tránsito, la transmisión de datos entre el usuario y el servidor puede ser interceptada fácilmente.
5. Indisponibilidad del sistema de información por saturación (Accidental)	Falta de configuración para atender determinado número de solicitudes y no se cuenta con un activo que brinde redundancia.	Interrupción de servicio del aplicativo por sobre carga de solicitudes de usuarios.	4	Alta	No haber desarrollado el sistema para atender un elevado número de solicitudes de usuarios y que este no tiene redundancia, ha ocasionado que el sistema quedara indisponible por periodos de 15 minutos, en los días recientes del lanzamiento de la aplicación. Además del monitoreo del tráfico de la red se observó que son solicitudes legítimas. Dado el contexto y el número de registros que podrían hacerse es muy probable que el incidente se repita en ocasiones, si se sobrepasan cierto número de solicitudes.

46 Este caso es particular, toda vez que, por la descripción del antecedente, si bien no se tiene registro de humedad en el lugar, la amenaza ya está presente (es visible la humedad) por lo que el escenario de vulneración está latente y se materializaría si no se atendiera pronto.

6. Negación de acciones (posible ataque DDoS) (Deliberada)	Falta de configuración de detección y bloqueo a paquetes maliciosos.	Interrupción de servicio del aplicativo por sobrecarga de solicitudes maliciosas.	**3**	**Media**	No configurar la detección y bloqueo de paquetes maliciosos en el sistema a partir del monitoreo del tráfico de información puede ocasionar una falta de disponibilidad del aplicativo por la cantidad de solicitudes de conexión malintencionadas. Sin embargo, al momento se ha detectado tráfico malicioso en la red, pero no se ha materializado la vulneración.[46]

Tabla 13. Ejemplo de valoración de la probabilidad de acuerdo con el ejemplo práctico. Autoría propia

Es importante precisar que los valores de probabilidad en el presente ejemplo práctico se otorgan de manera subjetiva, de acuerdo con los registros y la información con la que se cuenta, y de acuerdo con el conocimiento del contexto, pero es deseable que se consulte a expertos.

El impacto debe entenderse como aquella consecuencia negativa que afecta al activo, al sujeto obligado y a las personales titulares de los datos personales, como producto de la materialización del riesgo en un activo o un conjunto de activos de la entidad.

Es importante comprender que **el derecho a la protección de datos personales se trata de un derecho fundamental**, y por lo tanto **el impacto debe analizarse por cuanto a los daños o afectaciones a las personas titulares de datos personales en primera instancia**, no así la afectación a la organización o al sujeto obligado en sus recursos, que si bien importa y afecta, no es el fin último y propósito de un Sistema de Gestión de Seguridad de los Datos Personales[48].

Para mayor claridad se propone el siguiente ejemplo:

El impacto como la probabilidad deberán tener la misma escala o mismo rango cuantitativo. En este caso se valorará en 5 escalas, donde 1 será un impacto insignificante, 2 será menor o bajo, 3 será crítico o medio, 4 será grave y 5 muy grave.

Ahora bien, la valoración del impacto en la confidencialidad, en la integridad y en la disponibilidad también deberá valorarse en esa misma escala, y para sacar un valor único se estimará el promedio de las tres, a efecto de tener un valor único del impacto.

47 Al tratarse probablemente, de un ataque deliberado que puede depender de muchos factores como puede ser un ciber atacante, es más complejo otorgar un valor a la probabilidad puesto que no sabemos las intenciones y el momento en que lo realice.

48 Aunado a ello, el análisis y valoración del activo y las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad ya fue analizado en el inventario de activos, específicamente en la valoración de los activos, por lo que en este caso solo debe valorarse el impacto con un enfoque exclusivamente a los datos personales y por lo tanto a las personas titulares.

Impacto	Propiedad de la Seguridad		
	Confidencialidad	Integridad	Disponibilidad
1-Muy bajo	La pérdida de confidencialidad genera un impacto muy bajo o casi nulo en las personas titulares. Por ejemplo: La vulneración afectaría datos personales que ya son públicos.	La pérdida de integridad genera un impacto muy bajo o casi nulo en las personas titulares. Por ejemplo: se perdió la completitud de cierta información almacenada en el activo, pero no es información prioritaria, ni sensible.	La pérdida de disponibilidad genera un impacto muy bajo o casi nulo en las personales titulares. Por ejemplo: la disponibilidad se pierde sin que tenga efectos o consecuencias, ya que no se requiere tener a disposición los datos personales para algún trámite trascendente, sino solo para cuestiones administrativas o internas.
2-Bajo	La pérdida de confidencialidad genera un impacto bajo en las personas titulares. Por ejemplo: La pérdida de confidencialidad puede generar la pérdida de control de algunos datos personales no sensibles, pero que puede causar molestia y quizá el que deba realizar ajustes en cuestiones de contraseñas para salvaguardar la confidencialidad.	La pérdida de integridad genera un impacto bajo en las personas titulares. Por ejemplo: la pérdida de integridad de la información puede generar molestia e irritabilidad, así como el esfuerzo de volver a entregar la información completa porque se perdió una parte.	La pérdida de disponibilidad genera un impacto bajo en las personales titulares. Por ejemplo: puede generar molestia e irritabilidad a las personas titulares porque la falta de disponibilidad del activo retrasó un trámite no indispensable.
3-Medio	La pérdida de confidencialidad genera un impacto medio en las personas titulares. Por ejemplo: es posible que la pérdida de confidencialidad conlleve pérdidas económicas no significativas para las personas titulares, o bien cause preocupación a las personas y un esfuerzo medio para solucionar.	La pérdida de integridad genera un impacto medio en las personas titulares. Por ejemplo: es posible que la pérdida de integridad de la información cause problemas en una valoración, como cuando se introduce por error un nombre incorrecto pero existente en un registro de morosos o bien, por error en los datos, se le niega un servicio o un crédito a una persona.	La pérdida de disponibilidad genera un impacto medio en las personales titulares. Por ejemplo: la pérdida de disponibilidad del activo causa un retraso considerable en un trámite importante de las personas titulares, lo que les causa retraso en la obtención de una prestación o servicio.
4-Alto	La pérdida de confidencialidad genera un impacto alto o significativo en las personas titulares. Por ejemplo: la pérdida de confidencialidad en el activo conlleva pérdidas económicas o patrimoniales significativas, o implica la pérdida de control de datos personales de personas menores de edad o de datos sensibles, o bien, deja en desventaja o causa mayor discriminación a personas en situaciones de vulnerabilidad.	La pérdida de integridad genera un impacto alto o significativo en las personas titulares. Por ejemplo: La pérdida de integridad de la información puede conllevar la suspensión de un derecho, o bien un diagnóstico de salud erróneo que pueda dañar la integridad física o psicológica de las personas.	La pérdida de disponibilidad genera un impacto alto o significativo en las personales titulares. Por ejemplo: la pérdida de disponibilidad del activo causa un retraso considerable en un trámite o ejercicio de derechos indispensables, lo que puede dejar a una persona en una situación de vulnerabilidad.

5-Muy alto	La pérdida de confidencialidad genera un impacto muy alto en las personas titulares. Por ejemplo: la pérdida de confidencialidad en el activo conlleva pérdidas económicas o patrimoniales significativas, e implica la pérdida de control de datos personales sensibles de personas menores de edad o de personas en situación de vulnerabilidad que les perjudique aún más, causando, por ejemplo, doble o triple grado de discriminación o riesgos muy graves en su vida, integridad, y daños psicológicos muy graves.	La pérdida de integridad genera un impacto muy alto en las personas titulares. Por ejemplo: La pérdida de integridad de la información puede conllevar la suspensión de un derecho, o bien un diagnóstico de salud erróneo que pueda dañar la vida de las personas incluyendo personas menores de edad.	La pérdida de disponibilidad genera un impacto muy alto en las personales titulares. Por ejemplo: La falta de disponibilidad en los activos de información puede retrasar procesos o trámites que de no realizarse de inmediato puedan dañar la vida o integridad física o psicológica de personas titulares, incluyendo a las menores de edad.

Tabla 14. Ejemplos de criterios de impacto por cada propiedad de la información
Autoría propia

Una vez elaborado el análisis del impacto por cada propiedad de la información se debe obtener un valor único, por ejemplo, promediando el valor de las tres, donde la escala final será en los mismos niveles: 1 muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto.

Ejemplo de escala de impacto:

Impacto	
Cualitativo	Cuantitativo
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

Tabla 15. Ejemplo de escala de impacto

Ejemplo de aplicación de los criterios de impacto en el análisis de riesgos:

Activo	Escenario de vulneración	Impacto			
		C	I	D	Impacto total
Sistema electrónico RENMS-BBDD	1. Indisponibilidad de todos los servicios y activos que utilizan energía, por interrupciones del servicio de suministro eléctrico.	**1** La interrupción del sistema no afecta la confidencialidad de la información, por lo tanto, no se afecta esa esfera de la persona titular.	**1** La interrupción del suministro eléctrico no afecta la integridad de los datos personales.	**2** El escenario de vulneración está directamente relacionado con la disponibilidad. De acuerdo con la probabilidad de ocurrencia y el tiempo en que el registro está indisponible, puede representar para las personas titulares causa de molestia e irritación por no poder registrarse, o retrasarles el trámite, sin embargo, no se considera que en lo general se les deje en situación de vulnerabilidad o genere consecuencias graves.	**1.3=1- Muy bajo**
	2. Indisponibilidad del aplicativo por humedad.	**1** En caso de que el servidor se destruya por la humedad, este escenario no perjudica a la confidencialidad, en tanto que no se accede indebidamente a los datos personales, por lo tanto, no se daña a la persona titular.	**1** Este escenario no perjudica a la confidencialidad, en tanto que no se transgrede la integridad de los datos personales.	**4** El escenario de vulneración está directamente relacionado con la disponibilidad. En este caso debemos prever la destrucción del servidor por la humedad, por lo que se pierde totalmente la disponibilidad, lo que puede causar problemas en cuanto a la prestación del servicio de registro, dejando a muchas personas titulares menores de edad, quizá sin poder registrarse y retrasando los trámites y procesos, quizá por un tiempo considerable.	**2 Bajo**
	3. Accesos no autorizados por terceros e indebido tratamiento de datos personales por personas autorizadas; ello, por no contar con una política de gestión de perfiles y privilegios, y no controlar las copias generadas a la BBDD.	**5** El hecho de que muchas personas puedan acceder a la base de datos sin un control, y que puedan descargar la información del registro, puede dañar gravemente a las personas titulares, que, en gran medida, son menores de edad; esto, ya que se pueden divulgar los datos personales, poniendo en riesgo su integridad física y psicológica, más aún en el caso de las personas que tienen alguna discapacidad.	**5** Si gran cantidad de personas puede acceder a la base de datos sin gestionar los privilegios, es decir, si pueden generar copias, modificar la información, o eliminarla, es muy posible que por negligencia, error, o intencionadamente puedan modificarla, eliminar parte, y por lo tanto podrían causar consecuencias importantes a los titulares como, retrasar el trámite, no registrarlo por no registrar el nombre o los datos correctos.	**1** La falta de gestión de privilegios no afecta directamente a la disponibilidad.	**3.6=3- Alto**

	4. Acceso no autorizado, uso indebido de los datos personales, porque no se cuentan con protocolos de intercambio seguro de información.	**5** No contar con protocolos de intercambio seguro de información como el cifrado, hace posible que cualquier persona con mediano conocimiento pueda interceptar la información y utilizarla para sus propios fines. Así, al ser información de personas menores de edad, y en algunos casos, datos sensibles como discapacidades y datos de salud, pueden poner en una situación de vulnerabilidad grave a las personas titulares.	**5** No contar con protocolos de intercambio seguro de información como el cifrado, hace posible que cualquier persona con mediano conocimiento pueda interceptar la información y modificarla o alterarla, para cualquier fin. En ese sentido, es posible que se modifiquen o alteren datos de personas menores de edad, y en algunos casos datos sensibles, aunado a ello, se pueden causar consecuencias legales por la modificación de los datos.	**1** Este escenario no impacta directamente en la disponibilidad de los activos ni servicios, por lo que no afecta en este aspecto a las personas titulares.	**3.6=4- Alto**
	5. Pérdida de disponibilidad en el aplicativo por una gran cantidad de solicitudes legítimas, y no se cuenta con un servidor o una aplicación redundante.	**1** El escenario de pérdida de disponibilidad del aplicativo por no estar configurado para recibir determinado número de solicitudes o bien, porque no tiene la capacidad para procesarlas, no es un incidente que comprometa la confidencialidad, por lo que no afecta a las personas titulares en ese aspecto.	**1** No es un incidente que comprometa la integridad.	**2** Este escenario incide directamente en la disponibilidad, al no poder procesar determinado número de solicitudes el servidor se reinicia quedando indisponible por un tiempo. A pesar de ser grave para la Institución, este escenario no afecta significativamente a las personas titulares, sin embargo, puede causar molestias por el retraso del trámite.	**1.3=1 Muy bajo**
	6. Posible ataque DoS, que puede ocasionar una falta de disponibilidad del aplicativo por la cantidad de solicitudes de conexión malintencionadas.	**1** Este escenario no compromete la confidencialidad, puesto que se trata de peticiones malintencionadas que pueden afectar la disponibilidad de un activo y por lo tanto de un servicio.	**1** Este escenario no compromete la integridad.	**5** Este escenario compromete directamente la disponibilidad del activo, y por lo tanto puede afectar a las personas en cuanto al tiempo para realizar el registro, , en este supuesto también importa que no se cuenta con redundancia, por lo que si deja de operar este aplicativo no es posible que otro aplicativo asuma el servicio.	**2.3=2 Bajo**

Tabla 16. Ejemplo de análisis del impacto de los escenarios de vulneración del RENMS. Autoría propia

Finalmente, para concluir el análisis de riesgos se deberá estimar el riesgo cuantitativo y/o cualitativamente, realizando la multiplicación de los valores la probabilidad por el valor final del impacto.

El nivel de riesgo también debe ser representado en una escala cuantitativa y

cualitativa, se recomienda mantener la misma escala de valores, en este caso una escala de 5 niveles, en orden creciente y su equivalencia cuantitativa (1, 2, 3, 4 y 5) respectivamente, donde 1 será riesgo muy bajo; 2, bajo; 3, medio; 4, alto y 5 muy alto.

Ejemplo de escala para el riesgo:

Nivel de riesgo	
Cualitativo	Cuantitativo
Muy bajo	1-2
Bajo	3-4
Medio	5-9
Alto	10-16
Muy Alto	17-25

Tabla 17. Ejemplo de escala de riesgo

Para facilitar la visualización, es recomendable utilizar también una matriz de riesgos o mapa de calor. Ejemplo de matriz de riesgos de acuerdo con los criterios establecidos:

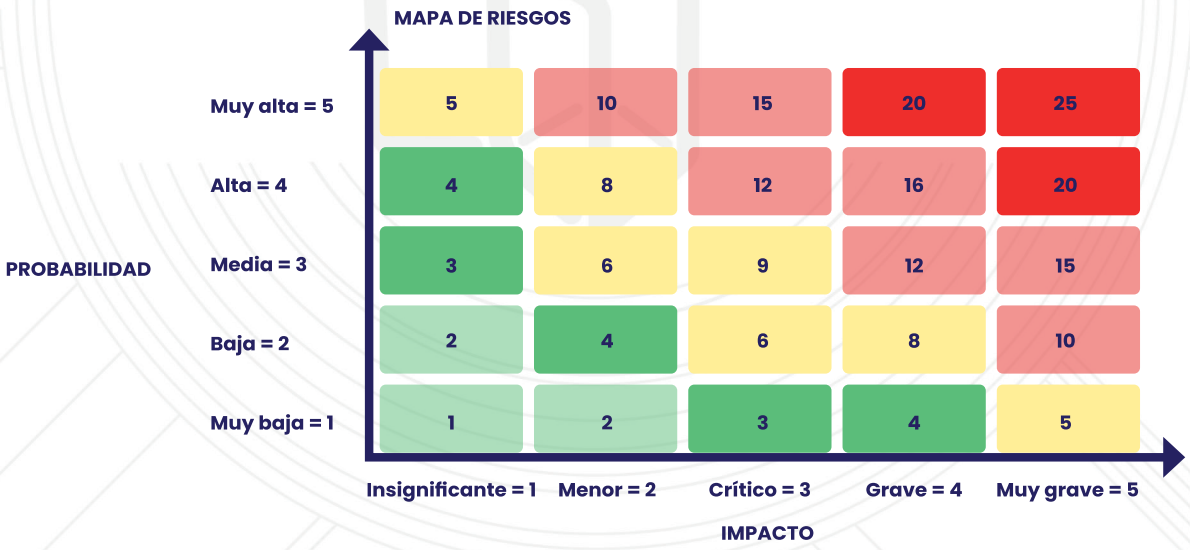


Figura 9. Ejemplo de matriz de riesgo
Autoría propia

De esta manera el sujeto obligado deberá identificar el valor para el impacto y la probabilidad de ocurrencia del incidente para obtener un valor que sea la base de la creación de escenarios de vulneración, la escala recomendada es la siguiente:

IMPACTO		PROBABILIDAD		NIVEL DE RIESGO	
Cuantitativo	**Cualitativo**	**Cuantitativo**	**Cualitativo**	**Cuantitativo**	**Cualitativo**
5	Muy alto	1	Muy baja	5	Medio
5		2	Baja	10	Alto
5		3	Media	15	Alto
5		4	Alta	20	Muy alto
5		5	Muy alta	25	Muy alto
4	Alto	1	Muy baja	4	Bajo
4		2	Baja	8	Medio
4		3	Media	12	Alto
4		4	Alta	16	Alto
4		5	Muy alta	20	Muy alto
3	Medio	1	Muy baja	3	Bajo
3		2	Baja	6	Medio
3		3	Media	9	Medio
3		4	Alta	12	Alto
3		5	Muy alta	15	Alto
2	Bajo	1	Muy baja	2	Muy bajo
2		2	Baja	4	Bajo
2		3	Media	6	Medio
2		4	Alta	8	Medio
2		5	Muy alta	10	Alto
1	Muy bajo	1	Muy baja	1	Muy bajo
1		2	Baja	2	Muy bajo
1		3	Media	3	Bajo
1		4	Alta	4	Bajo
1		5	Muy alta	5	Medio

Tabla 18. Multiplicación de los valores posibles de probabilidad e impacto en la escala definida. Autoría propia

Ejemplo práctico:

Activo	Escenarios de vulneración	Impacto				Probabilidad	Riesgo inherente
		C	I	D	Impacto total		
Sistema electrónico RENMS-BB-DD	**1. Indisponibilidad de todos los servicios y activos que utilizan energía, por interrupciones del servicio de suministro eléctrico.**	1	1	2	1.3=1-Muy bajo	3	3-Bajo
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • Falta de disponibilidad del sistema por tiempos no muy prolongados. • Retraso en los procesos internos, y en el trámite del registro • Pérdida de confianza en una Institución fundamental del Estado						
Sistema electrónico RENMS-BB-DD	**2. Indisponibilidad del aplicativo por humedad.**	1	1	4	2-Bajo	3-Media	6-Medio
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • Falta de disponibilidad del sistema por tiempos inciertos en caso de que se destruya el activo. • Probable pérdida de información no recuperable, por lo que se tendría que solicitar nuevamente. • Retraso de procesos internos y por lo tanto de trámites por un tiempo probablemente prolongado. • Pérdida de confianza en una Institución fundamental del Estado						
Sistema electrónico RENMS-BB-DD	**3. Accesos no autorizados por terceros e indebido tratamiento de datos personales por personas autorizadas; ello, por no contar con una política de gestión de perfiles y privilegios, y no controlar las copias generadas a la BBDD.**	5	5	2	4-Alto	5- Muy alto	20-Muy Alto
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • Pérdida irreversible del control de los datos personales de personas menores de edad, que en algunos casos puede incluir datos sensibles. • La divulgación de los datos personales puede traer consecuencias como discriminación a las personas titulares, dentro de las que se encuentran menores de edad.						

Activo	Escenarios de vulneración	Impacto				Probabilidad	Riesgo inherente
		C	I	D	Impacto total		
Sistema electrónico RENMS-BB-DD	**4. Acceso no autorizado, uso indebido de los datos personales, porque no se cuentan con protocolos de intercambio seguro de información.**	5	5	1	3.6=4-Alto	5-Muy alta	20-Muy alto
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • Pérdida de control irreversible de los datos personales de personas menores de edad, que en algunos casos puede incluir datos sensibles. • Terceros no autorizados pueden hacer uso indebido de la información como divulgarla. • La divulgación de los datos personales puede traer consecuencias como discriminación a las personas titulares, dentro de las que se encuentran menores de edad y menores de edad con discapacidad.						
Sistema electrónico RENMS-BB-DD	**5. Pérdida de disponibilidad en el aplicativo por una gran cantidad de solicitudes legítimas, y no se cuenta con un servidor o una aplicación redundante.**	1	1	2	1.3=1-Muy bajo	4-Alta	4-Bajo
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • Falta de disponibilidad del sistema sin saber el tiempo en el que volverá a estar operable, retrasando el tiempo del proceso interno y de trámite. • Pérdida de confianza en una Institución fundamental del Estado.						
Sistema electrónico RENMS-BB-DD	**6. Posible ataque DoS, que puede ocasionar una falta de disponibilidad del aplicativo por la cantidad de solicitudes de conexión malintencionadas.**	1	1	5	2.3=2-Bajo	3-Media	6-Medio
	Análisis de impacto en los titulares De materializarse el escenario de riesgo, algunas consecuencias para las personas titulares son: • alta de disponibilidad del sistema por tiempos indefinidos, lo que cause retraso en los procesos internos y retrasos en el trámite de registro. La afectación a las personas titulares no se considera grave. • Pérdida de confianza en una Institución fundamental del Estado						

Tabla 19. Ejemplo de análisis del riesgo inherente
Autoría propia

Evaluación del riesgo

Una vez realizado este análisis, se deberá evaluar el riesgo, comparando el nivel del riesgo inherente resultado del análisis de riesgos con el criterio de riesgo aceptable para el sujeto obligado, a fin de priorizar el tratamiento.

Ejemplo:

Activo: RENMS BBDD							
	Impacto						
Escenario de vulneración	C	I	D	Impacto total	Prob.	Riesgo inherente	Evaluación
1. Indisponibilidad de todos los servicios y activos que utilizan energía, por interrupciones del servicio de suministro eléctrico.	1	1	2	1.3=1-Muy bajo	3-Media	3-Bajo	Riesgo aceptable
2. Indisponibilidad del aplicativo por humedad.	1	1	4	2-Bajo	3-Media	6-Medio	Riesgo no aceptable
3. Accesos no autorizados por terceros e indebido tratamiento de datos personales por personas autorizadas; ello, por no contar con una política de gestión de perfiles y privilegios, y no controlar las copias generadas a la BBDD.	5	5	2	4-Alto	5Muy alta	20-Muy alto	Riesgo no aceptable
4. Acceso no autorizado, uso indebido de los datos personales, porque no se cuentan con protocolos de intercambio seguro de información.	5	5	1	3.6=4-Alto	5-Muy Alta	20-Muy alto	Riesgo no aceptable
5. Pérdida de disponibilidad en el aplicativo por una gran cantidad de solicitudes legítimas, y no se cuenta con un servidor o una aplicación redundante.	1	1	2	1.3=1-Muy bajo	4-Alta	4-Bajo	Riesgo aceptable

Activo: RENMS BBDD							
	Impacto						
Escenario de vulneración	C	I	D	Impacto total	Prob.	Riesgo inherente	Evaluación
6. Posible ataque DoS, que puede ocasionar una falta de disponibilidad del aplicativo por la cantidad de solicitudes de conexión malintencionadas.	1	1	5	2.3=2-Bajo	3-Media	6-Medio	Riesgo no aceptable

Tabla 20. Ejemplo de valoración del riesgo inherente
Autoría propia

De acuerdo con el ejemplo, el sistema electrónico RENMS-BDD es un activo crítico del sujeto obligado, y en el caso particular los escenarios de riesgo relativos al acceso a la información por personal no autorizado debido a la falta de gestión de perfiles y privilegios, y el acceso y uso indebido por personas no autorizadas, debido a la falta de protocolos de seguridad en la transmisión de la información(riesgos muy altos), deben priorizarse en el tratamiento del riesgo dadas las graves consecuencias que puede causar a las personas titulares, posteriormente deben programarse los trabajos para atender los riesgos medios, en este caso, la humedad en el centro de datos donde se encuentra el servidor, así como la falta de disponibilidad por sobrecarga de solicitudes maliciosas. Finalmente, el que un riesgo sea bajo, no quiere decir que no sea posible y que no afecte en absoluto, por lo que deberá mantenerse monitoreado y establecer en la medida de lo posible actividades para atenderlos y saber actuar si llegan a materializarse.

Una vez evaluados los riesgos, se tendrá un panorama claro para tomar mejores decisiones y administrar mejor los recursos del sujeto obligado, que son finitos.

En ese sentido, habiéndolos priorizado los riesgos, se debe analizar ¿Qué acciones debemos emprender para tratar ese riesgo?

5.2 Tratamiento del riesgo: Identificación de las medidas de seguridad (análisis de brecha)

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas más adecuadas para llegar a los objetivos de nivel de riesgo aceptable planteado. Para ello se deberá elegir la opción de tratamiento de riesgo idónea y que más convenga al sujeto obligado.

El tratamiento de los riesgos implica identificar el rango de opciones para ocuparse de estos, evaluar esas opciones y preparar planes para dicho tratamiento e implementarlos en la siguiente fase.

En ese sentido, el tratar un riesgo implica decidir:

- Mitigarlo o reducirlo,
- Retenerlo,
- Evitarlo,
- Compartirlo
- Aceptarlo

Opciones de Tratamiento de Riesgo

1. Reducir el Riesgo

Reducir el riesgo implica seleccionar y aplicar los controles, medidas de seguridad o salvaguardias apropiadas para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.

Durante la selección de controles o medidas es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles o medidas de seguridad 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.

2. Retener el Riesgo

Esta actividad describe que no se cuenta con la suficiente información para identificar medidas de seguridad para conocer como trabajar con el riesgo, por lo que, es necesario aislar los activos comprometidos a fin de hacerse con la información necesaria para reducir el riesgo, es así que, la retención del riesgo habla sobre la contención del riesgo para su analisis, retener la responsabilidad por las pérdidas de los activos a causa de la materialización del riesgo, en este caso, supone asumir la responsabilidad del impacto que puede generar lo anterior en la operación del sujeto obligado y probablemente en los derechos y libertades de las personas titulares de los datos personales en tanto se busca implementar otra opción de tratamiento del 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 necesi-

dad 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.

Esta opción de tratamiento supone en principio un riesgo no aceptable para la entidad, el cual puede retenerse temporalmente, mientras se cuenta con los medios y recursos para atenderlo, es importante que dicha decisión sea comunicada y aceptada por los Órganos Directivos del sujeto obligado y el Comité de Transparencia.

3. **Evitar el Riesgo**

Se refiere a la decisión de no verse involucrado en una situación de riesgo. Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios, es recomendable evitar el riesgo; esto, si de acuerdo con el contexto del sujeto obligado es posible, 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 centro de datos a una ubicación donde no exista el mismo riesgo o que se pueda mantener bajo control.

4. **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 sus posibles efectos, por ejemplo, al contratar un seguro o un proveedor que administre la seguridad del sujeto obligado.

En algunas ocasiones las organizaciones deciden contratar seguros contra riesgos, donde una entidad aseguradora asume los costos de la degradación de los activos y las pérdidas económicas que pueda generar la materialización de dicho riesgo, sin embargo, cuando un sujeto obligado comparte un riesgo, no se comparte la responsabilidad, es decir, la entidad no deja de ser responsable del tratamiento de los datos personales, y de darse un incidente de seguridad que los afecte, será el sujeto obligado quien debe responder frente a los titulares, además, es importante que se considere que involucrar a un nuevo actor en los procesos del responsable siempre representa un riesgo que debe ser analizado.

Aceptación del Riesgo

Aceptar el riesgo quiere decir que el responsable del tratamiento decide aceptar las consecuencias y probabilidad de un riesgo en particular.

Esta opción se puede tomar en dos supuesto, el primero (el ideal), porque se ha trabajado para reducir el riesgo a un nivel aceptable para la entidad (criterio de Nivel de Riesgo Aceptable establecido en la metodología de gestión de riesgos), y por lo tanto a partir de ahí solo se buscará mantenerlo monitoreado; o bien,

cuando los costos de implementación de una medida de seguridad sobrepasan el valor del activo que se desea proteger o es imposible implementar las medidas de seguridad correspondientes para su reducción; en ambos casos la organización asume los daños provocados por la materialización del riesgo incluso para las personas titulares y las responsabilidades que ello conlleva.

Esto significa que, dentro del tratamiento del riesgo, la entidad deberá ceñirse a lo establecido en la metodología, particularmente lo que refiere al Nivel de Riesgo Aceptable (que se recomienda que sea bajo o muy bajo en tanto que estamos en materia de derechos fundamentales y el impacto afecta a personas titulares), no obstante, es posible que, por causas como la falta de recursos económicos, administrativos o humanos deba aceptarse un riesgo de mayor nivel, lo cual se recomienda sea excepcional, y de ser así, será importante que se documente y sea aprobado por el o los propietarios del tratamiento, o el titular del área, por el Comité de Transparencia y de ser posible por alguna persona miembro de Órganos Directivos u Órganos de Gobiernos de la entidad, a efecto de que el responsable del tratamiento está aceptando un riesgo distinto al establecido en los criterios para la gestión del riesgo.

Finalmente, para efectos de la comprensión del riesgo, es importante reiterar que el riesgo cero no existe, por lo que se buscará mitigarlo a un nivel aceptable (bajo o muy bajo) y dentro del plan de monitoreo y revisión deberán constar las acciones para supervisar dichos riesgos.

Lo que se busca en el tratamiento de los riesgos es que las consecuencias adversas de los riesgos se reduzcan lo más razonablemente posible con independencia de cualquier criterio absoluto, por ejemplo, se deben considerar los riesgos que son casi imposibles que ocurran (es decir la probabilidad es muy baja) pero que, de suceder, serían catastróficos (en la teoría denominados "cisne negro"[49]), en cuyo caso sería sumamente costoso mantener medidas de seguridad, sin embargo, se deben implementar controles de monitoreo y vigilancia en tanto que la probabilidad de que sucedan es remota, pero de suceder, serían fatales en cuanto impacto en este caso tanto para la entidad como para las personas titulares de los datos.

Ahora bien, los cuatro tipos de tratamiento de riesgo no son mutuamente excluyentes. Los sujetos obligados pueden beneficiarse sustancialmente de la combinación de opciones, quizá primero se requiere retener un riesgo mientras se solicita el presupuesto o los recursos para implementar medidas de seguridad adecuadas, para después trabajar en su implementación hasta lograr la reducción a niveles aceptables. La decisión que se tome se materializará a través de los controles, medidas o salvaguardas de seguridad, que se verán adelante.

49 Taleb, Nicholas Nassim. El cisne negro, el impacto de lo altamente improbable, 2007, EUA, Editorial Paidós. Investopedia https://www.investopedia.com/terms/b/blackswan.asp

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 respecto a la gestión del riesgo, 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 en el sujeto obligado
- Informar sobre las funciones y obligaciones, roles y responsabilidades que tiene cada persona como parte activa del SGSDP
- 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 custodios y a las partes interesadas sentido de responsabilidad (diligencia) sobre el riesgo
- Incrementar la conciencia del riesgo en la organización

La coordinación entre las personas designadas para tomar las decisiones y las partes involucradas es indispensable para la toma de decisiones, el sujeto obligado puede desarrollar planes o protocolos de comunicación del riesgo que involucren a personas que desempeñen roles fundamentales en la seguridad de los datos personales, en conjunto con el Comité de Transparencia y en su caso, el oficial de protección de datos personales, donde pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación, en momentos donde la operación del riesgo sea normal pero también en casos de emergencia para responder, por ejemplo, a los incidentes de seguridad o vulneraciones y las obligaciones legales que estas conllevan como la notificación a los titulares y en su caso, al Instituto y a los Organismos Garantes[50].

50 Se debe recordar que el artículo 40 establece la obligación del responsable de notificar al Instituto y a los Organismos Garantes, según corresponda, las vulneraciones a la seguridad de los datos personales que afecten significativamente derechos morales o patrimoniales de las personas titulares. Por su parte los artículos 66 y 67 de los Lineamientos Generales establecen el plazo, y lo que debe contener dicha notificación.

El siguiente esquema representa la gestión de riesgos y establece claramente la relación entre el análisis de riesgos y el tratamiento del riesgo para mejor entendimiento.

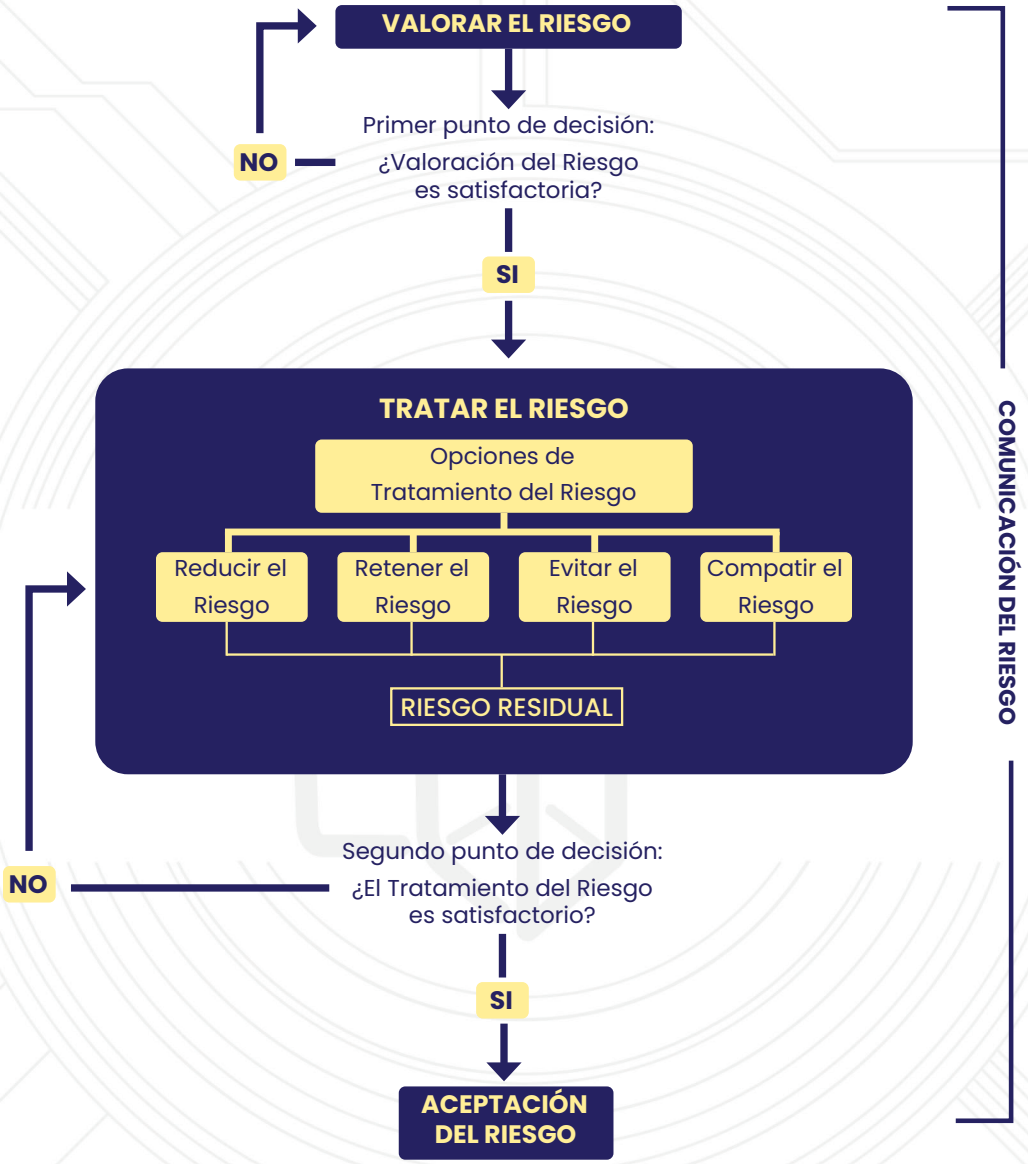


Figura 10. Esquema de tratamiento del riesgo[51]

De igual forma, el artículo 41 de la Ley General, prevé informar a las personas titulares respecto de las vulneraciones ocurridas a sus datos personales, se debe recordar que el artículo 41 establece el contenido de dicha comunicación a efecto de a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos. El artículo 68 de los Lineamientos Generales establece los contenidos mínimos del informe y de las acciones previas a realizar por el responsable.

51 INAI, Mayo de 2024, Guía de apoyo para la elaboración del Documento de Seguridad. p68. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf

Entender las opciones de tratamiento de riesgo, así como la comunicación hará más claro entender el análisis de brecha y la operación del SGSDP en lo general.

Análisis de brecha

El análisis de brecha como contenido del Documento Seguridad en relación con un Sistema de Gestión de Seguridad de Datos Personales, conjunta varias actividades en la etapa del tratamiento del riesgo, ya que es cuando se debe decidir qué hacer con el nivel de riesgo detectado; sin embargo, para llegar a esa decisión se deben elaborar varios análisis, entre ellos el análisis de riesgo residual, aunado a:

- Las medidas de seguridad existentes y efectivas;
- Las medidas de seguridad faltantes, y
- La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

Artículo 33.
"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:
(...)
V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
(...)"

"Análisis de brecha
Artículo 61. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:
I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

El análisis de brecha es el examen que se realiza sobre las medidas de seguridad con la que ya se cuenta, evaluar si estas son efectivas; determinar las que faltan, de las que faltan cuáles son viables para implementarse, y de las que se tienen cómo se podrían fortalecer.

Recordemos que para este punto ya hemos elaborado el análisis y la evaluación del riesgo, por lo que hemos obtenido el riesgo inherente de los activos, sin embargo, es muy común y probable que dentro de la entidad ya existan algunas medidas de seguridad implementadas, por lo que una vez elaborada la primera fase del análisis de brecha (identificación de las medidas existentes) para eva-

luar su eficacia, será importante realizar una nueva iteración del análisis de riesgos, esta vez valorando el riesgo residual, es decir, esta vez restando los valores de la eficacia de la medida de seguridad implementada, asimismo, deberá considerarse y planearse la evaluación del nivel de madurez de la medida dentro de la entidad, en este caso una evaluación de una medida que quizá no está bien implementada, aunque la evaluación real se hará hasta la siguiente iteración de análisis de riesgos, en la fase de monitoreo, para evaluar un rango establecido si está documentada y operando, esto nos dará el panorama actual de cómo se tratan los riesgos de seguridad de los datos personales en el sujeto obligado

En ese sentido, una vez obteniendo el riesgo residual, y habiendo elegido las opciones de tratamiento, es posible pasar a la siguiente fase que es determinar las medidas faltantes, para ello se requiere una base de comparación, como pueden ser los diversos catálogos de las metodologías de gestión de riesgos, o de los estándares internacionales enfocados a la seguridad de la información y a la privacidad; por ejemplo, el catálogo de controles de seguridad que se encuentra como anexo de la Guía del INAI para implementar un Sistema de Gestión de Seguridad de Datos Personales, de junio de 2015[52], o bien los controles del estándar ISO/IEC 27002:2022, el de la metodología MAGERIT 3.0[53] o el de alguna otra**.**

Es importante mencionar que no todos los controles le pueden aplicar a su sistema de tratamiento de información pues algunos, pueden no ser compatibles con el tipo de sistema en el que se encuentra la información. Por lo que de dichos catálogos de controles se deben elegir cuáles son aplicables e idóneos de implementar en lo general a toda la entidad para lo que es recomendable realizar una Tabla o Declaración de Aplicabilidad de los controles, la cual debe incluir los objetivos de control y controles seleccionados del estándar o de la metodología seleccionada(s), las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso[54].

Lo anterior sería importante para saber cuál será la meta de controles a alcanzar del Sistema de Gestión, así como en caso de querer certificarse en el estándar internacional, es un requisito indispensable para evaluar.

Ahora bien, independientemente de los controles seleccionados para implementarlos en la entidad, es importante mencionar desde ahora que, se deberá revisar cuales son los específicos que inciden en los escenarios de riesgo más críticos (obtenidos en el análisis de riesgos) y por lo tanto disminuyen el nivel de riesgo de los activos de apoyo y de información más críticos del sujeto obligado,

52 Guía disponible en https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

53 Puede consultar el catálogo en el siguiente enlace: https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf

54 En la práctica, cuando una organización se requiere certificar, los auditores solicitan la tabla denominada SoA, por sus siglas en ingles Statement of Applicability, en principio las organizaciones deben implementar múltiples controles de cada categoría de controles, y si por algún motivo alguno de los controles no aplica, se debe justificar exhaustivamente el por qué no aplica.

para así comenzar a trabajar su implementación antes que los demás, lo que se plasmará en el plan de trabajo.

Posteriormente, se deben determinar las medidas de seguridad o controles que se pueden reemplazar y por último cuáles se pueden fortalecer.

Con las medidas elegidas se debe volver a realizar una iteración al análisis de riesgos para obtener un probable riesgo residual (en este caso, el análisis es prospectivo, toda vez que, en algunos casos, no se sabrá con certeza si las medidas seleccionadas disminuyen realmente el riesgo, hasta que se ponga en operación el sistema de gestión y que suceda un incidente de seguridad que implique la operación de esa medida).

Particularmente para el fortalecimiento de las medidas, será importante planear una escala de madurez de las medidas de seguridad, que nos ayude a valorar el nivel de implementación dentro del sujeto obligado, adelante se presentará un ejemplo de escala de madurez, posterior al ejemplo de riesgo residual

Para el tratamiento del riego será imprescindible contar con la colaboración de los propietarios de los tratamientos, de los custodios, con algún representante de las unidades administrativas encargadas del presupuesto, así como de las áreas que están operando actualmente las medidas de seguridad existentes dentro del sujeto obligado, y el área de tecnologías de la información o similar, toda vez que se requerirá comprender qué medidas existen al momento, cómo están operando, y que se propongan nuevas de acuerdo con las posibilidades reales del sujeto obligado, esto es los recursos humanos, administrativos y los presupuestos con los que cuenta el área.

Resumiendo, para el tratamiento del riesgo (lo que incluye el análisis de brecha), se debe:

a) Analizar las medidas existentes al interior del sujeto obligado, para este análisis se requerirá evaluar su categoría, así como si las medidas son necesarias, idóneas y eficaces, si están cumpliendo el objetivo respecto a la decisión de tratamiento de riesgo tomada. Para ello, se deberá realizar una primera iteración del análisis de riesgos, esta vez obteniendo el riesgo residual, asimismo, deberá evaluarse el nivel de madurez de la medida dentro de la entidad. Esto nos dará una visión actualizada sobre el estado que guarda la seguridad de datos personales en el sujeto obligado.

b) Posteriormente, se debe realizar una búsqueda o investigación de las medidas de seguridad faltantes, para ello, se requiere una base de comparación, para lo cual es posible consultar los catálogos de medidas de seguridad, controles o salvaguardas con las que cuentan las distintas metodologías de gestión de riesgos, o bien, el estándar internacional ISO 27002, y analizar cuáles faltan de implementarse en el sujeto obligado, para lo que es recomendable realizar una tabla o declaración de aplicabilidad.

c) Del catálogo de controles o medidas, se deberán seleccionar las medidas idóneas de acuerdo con el contexto de la entidad, es decir, analizar si son

factibles de implementar, la forma en que se hará, el nivel de madurez con el que se comenzará a operar, y la evaluación sobre si reduce el riesgo (realizando una nueva iteración del análisis de riesgo residual de manera prospectiva[55]).

Identificación de las medidas de seguridad

Para identificar las medidas de seguridad tanto existentes como faltantes es importante contar con algún catálogo que describa los controles generales para poder identificar las medidas de seguridad particulares con las que cuenta el sujeto obligado.

Al respecto, en la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales de junio de 2015, del INAI, en el anexo D, contiene un catálogo de controles con descripción en el que es posible basarse. Lo anterior tomando en cuenta que dentro de las figuras de autoridad en el sector público está el Comité de Transparencia.

OBJETIVO DE CONTROL	DESCRIPCIÓN
Políticas de gestión de datos personales	Debe 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 l 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	

55 Solo se podrá confirmar que las medidas seleccionadas funcionen cuando se prueben, y esto es en la operación o puesta en marcha del sistema de gestión. Sin embargo, es un buen ejercicio ir midiendo que tanto se espera que funcione.

OBJETIVO DE CONTROL	DESCRIPCIÓN
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.
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.

Figura 11. Ejemplo de un Catálogo de controles de seguridad, autoría propia

Se recomienda elaborar una tabla con los controles, la descripción, así como las medidas de seguridad implementadas y las medidas de seguridad que se consideren idóneas para implementarse. O de algún catálogo agregar los controles, decidir si aplica o no aplica, si existe algún control implementado, y se podría implementar alguno ya sea para fortalecer o porque no existe ninguno respecto a la descripción del control.

Ejemplo:

SEGURIDAD DEL PERSONAL			
Objetivo del control Identificar responsabilidades de seguridad en cada puesto de trabajo			
Descripción 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.			
¿Se cuenta o no con algún control? ¿Cuál(es)?		**¿Se puede implementar alguno? ¿Cuál(es)? Recursos**	
SI ☐	NO ☐	SI ☐	NO ☐
Observaciones:			

Obtención del riesgo residual

Análisis de las medidas de seguridad acuerdo con su categoría.

De acuerdo con la Ley General encontramos tres tipos de medidas de seguridad: administrativas, físicas y técnicas.

Artículo 3.
"Para los efectos de la presente Ley se entenderá por:
(...)
XX. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XXI. **Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

XXII. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

> c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
> d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;
>
> XXIII. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
> a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
> b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
> c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
> d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;
> (...)"

Las medidas de seguridad administrativas se refieren a cuestiones organizacionales, como políticas, programas, proyectos y procedimientos que establecen lo que está permitido y lo que no, y la forma de organización en materia de protección de datos personales. Se debe comprender que "*estas no operan por sí mismas, sino que requieren de otras medidas que las pongan en práctica*"[56] por ejemplo la capacitación (medida administrativa también), y requieren ser monitoreadas. Las medidas físicas son aquellas con las que se busca resguardar los activos de forma física, es decir, *restringen el acceso corporal a los activos*[57]. Y finalmente las técnicas son las que utilizan la tecnología para resguardar la confidencialidad, integridad y disponibilidad de los activos.

Asimismo, existe otra categorización de acuerdo con distintas metodologías, que es importante a fin de comprender la función de la medida respecto a lo que hace respecto al riesgo, particularmente, si incide en la disminución de la probabilidad o el impacto, si detecta amenazas o vulnerabilidades, las previene, las corrige o disuade. En ese sentido, se dividen en:

- Correctivas
- Preventivas
- Disuasorias
- Detectivas

56 Corona Fraga, Pablo. Guía práctica para la gestión de riesgos en la era de la ciberseguridad. (julio 2019) Primera edición. México. Thomson Reuters. P. 90

57 Ibidem

Mediante el análisis de acuerdo con su categoría y función se puede advertir si éstas reducen el riesgo objetivamente. Por ejemplo, la medida de seguridad de control de accesos físicos es una medida de acuerdo a la ley, física, y por cuanto a su función preventiva y disuasoria, en tanto que la implementación debe ser previa a un incidente de seguridad para que funcione, es decir, no es reactiva o de recuperación, además de que es disuasoria en tanto que induce a las personas que conocen de la política de control de accesos a cambiar de opinión o a desistir de un propósito de indebido tratamiento de datos personales y a actuar con diligencia; por ello, esta medida reduce la probabilidad de ocurrencia, aunque no podemos controlar la voluntad de las personas, sin embargo es una medida que nos ayuda a controlar un poco la superficie de vulneración, pero, cuando una persona decide deliberadamente acceder para obtener la información, al materializarse el riesgo, aunque tengamos control de accesos físicos, no reduciría el impacto en los activos de información y por lo tanto, en las personas titulares de los datos personales afectados. Por lo tanto, la medida control de accesos físicos, solo reduce la probabilidad de ocurrencia.

En ese sentido para facilitar el análisis es importante retomar el procedimiento de análisis de riesgos y vincular el análisis de brecha a este, seleccionando aquellas medidas que ya están implementadas, y de ellas, revisar si alguna incide en alguno de los riesgos inherentes con los valores más altos.

Una vez vinculadas las medidas al riesgo, valorar si el control implementado reduce el impacto o reduce la probabilidad, a partir de ello se puede valorar el riesgo residual. El riesgo residual es la sustracción del riesgo inherente menos las medidas de seguridad implementadas.

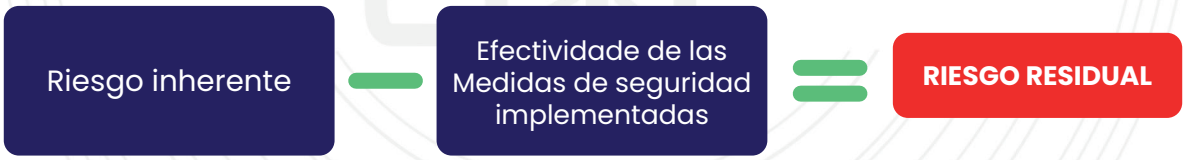


Tabla 12. Fórmula para la obtención del riesgo residual
Autoría propia

Ejemplo de la primera iteración del análisis de riesgos para la obtención del riesgo residual, considerando las medidas de seguridad ya implementadas respecto de los ejemplos de escenarios de vulneración para un activo:

En este caso se debe suponer que ya se identificaron ciertas medidas de seguridad que están implementadas (primera parte del análisis de brecha), posteriormente, se vinculan las medidas de seguridad implementadas que inciden en los riesgos más altos, y se realiza el análisis de riesgos esta vez restando los valores de efectividad (valores subjetivos) que consideremos por cada medida.

Para ello, debemos analizar la medida de seguridad:
Supongamos que, del análisis de brecha, en la identificación de medidas de seguridad, identificamos lo siguiente:

- Se habían implementado el uso de no break en los servidores.
- Se encuentran programadas ya las reparaciones de tuberías en todas las instalaciones del edificio.
- Se cuenta con una política general y gestión de perfiles con privilegios asignados por la naturaleza de sus funciones; y el custodio ha implementado dicha la política restringiendo la generación de copias, solo a perfiles administradores, y se tienen definidas los privilegios que puede realizar cada perfil dentro del RENMS.
- Se acaba de implementar el protocolo https para el intercambio seguro de información.
- Se cuenta con un servidor institucional que presta redundancia de todos los servicios.

ACTIVO: RENMS-BBDD										
Escenario de vulneración	**Impacto**									
	C	**I**	**D**	**Impacto total**	**Prob**	**Riesgo inherente**	**Control implementado**	**¿Reduce impacto?**	**¿Reduce probabilidad?**	**Riesgo residual**
1. Indisponibilidad de todos los servicios y activos que utilizan energía, por interrupciones del servicio de suministro eléctrico.	1	1	2	1.3=1	4	4-Bajo	Uso de no break[58] en los servidores	Sí. La medida sí reduce el impacto, pero en este caso está en el valor mínimo que se puede asignar. Impacto residual= 1	En principio esta salvaguarda no controla la probabilidad. Probabilidad residual= 2	2-Muy bajo

58 Un no break es un dispositivo que se instala en cualquier aparato que pueda disparar un disyuntor. A la primera señal de un problema, el no break desconectará el dispositivo para que sus disyuntores no tengan que hacerlo. Esto evita que se produzca un apagón.
Revista Seguridad 360º, 2022, octubre. ¿Qué es un No Break? La importancia de la protección eléctrica en su empresa, disponible en https://revistaseguridad360.com/destacados/que-es-un-no-break/ última fecha de consulta: 30/08/2023

ACTIVO: RENMS-BBDD										
Escenario de vulneración	**Impacto**									
	C	**I**	**D**	**Impacto total**	**Prob**	**Riesgo inherente**	**Control implementado**	**¿Reduce impacto?**	**¿Reduce probabilidad?**	**Riesgo residual**
Análisis de la medida en lo particular Esta medida pertenece a la categoría de seguridad física y medio ambiental, que busca prevenir daños e interferencias en la información y en los activos de apoyo. El no break es una medida particular de esta categoría que busca proteger a los activos de una falla eléctrica. Por lo tanto, es una medida preventiva. Y conforme a la categorización de la Ley General es una medida física. ¿Reduce impacto? Sí, esta medida busca que no se dañe el servidor y por lo tanto el RENMS al suscitarse el apagón de energía. Sin embargo, existe la posibilidad de que el no break falle, y si es así, el impacto será el mismo. Sin embargo, Aunque la medida de seguridad reduce el impacto, se recomienda que no baje de 1 y en ningún caso, la metodología permita reducir a cero, toda vez que el riesgo cero no existe, por lo tanto, tampoco el impacto ni la probabilidad. **¿Reduce probabilidad?** En principio esta salvaguarda no controla la probabilidad, ya que las interrupciones pueden ser causadas por diversas situaciones, quizá por una falla eléctrica que tenga que repararse con la compañía eléctrica. Sin embargo, si se pueden implementar controles para reducir e incluso evitar el daño a los activos cuando esas fallas se producen. Sin embargo, al no poder reducir el impacto porque está en el mínimo, se puede reducir la probabilidad, en tanto que al reducir el impacto se reduce la probabilidad de tener una interrupción de suministro eléctrico, y el escenario disminuye su probabilidad materialización, por lo que no debe afectar el funcionamiento del servidor, aunque persiste una probabilidad de que los no break no funcionen correctamente por diversos factores.									
2. Indisponibilidad del aplicativo por humedad.	1	1	4	2.3=2	3	6-Medio	Revisión y reparación de instalación hidráulica de los tramos de tubería que presenten filtrado de agua por deterioro.	Sí. Impacto residual=1.3-1	Sí. Aunque en principio no es una medida que reduzca la probabilidad de la amenaza que ya se está materializando si reduce la probabilidad de que suceda el riesgo posteriormente. Probabilidad residual=2	2-Muy bajo
Análisis de la medida en lo particular Esta medida pertenece a la categoría de seguridad física y medio ambiental, que busca prevenir daños e interferencias en la información y en los activos de apoyo. La reparación de tuberías es una medida particular de esta categoría que busca corregir la falla, en tanto que es una tubería que, por ser tan vieja, ha fallado. Por lo tanto, es una medida correctiva por el momento en que se presenta. Y conforme a la categorización de la Ley General es una medida física.										

ACTIVO: RENMS-BBDD										
Escenario de vulneración	Impacto				Prob	Riesgo inherente	Control implementado	¿Reduce impacto?	¿Reduce probabilidad?	Riesgo residual
	C	I	D	Impacto total						
¿Reduce impacto? Sí, en tanto que de acabarse la humedad no habría daño al servidor y por lo tanto no habría impacto. Sin embargo, debe considerarse una pequeña posibilidad de que la reparación falle. Por lo tanto, la confidencialidad y la integridad se mantienen en 1, y la disponibilidad reduce a 2, por lo que 1+1+2=4/3=1.3=3. Para el impacto se debe analizar cada una de las propiedades, en este caso la confidencialidad se mantiene puesto que el escenario no la transgrede, de igual forma a la integridad; y finalmente la disponibilidad si reduce, puesto que al repararse las filtraciones debería desaparecer el escenario de riesgo y por lo tanto no se daña el servidor, en este caso se reduce a 2, porque existe una posibilidad de que la reparación no sea suficiente o no se haga correctamente. **¿Reduce la probabilidad?** No, como se explicó es una medida correctiva en tanto que la humedad ya está presente, en caso de que se hicieran revisiones periódicas de prevención, reduce la probabilidad, en este caso se busca corregir. Ahora bien, al hacerse la reparación actúa a su vez como medida preventiva a futuro y se elimina la causa del escenario de vulneración, aunque debe preverse un pequeño porcentaje de probabilidad de que la reparación no se realice correctamente; por ello en este caso se decidió reducir a 2.										
3. Accesos no autorizados por terceros e indebido tratamiento de datos personales por personas autorizadas; ello, por no contar con una política de gestión de perfiles y privilegios, y no controlar las copias generadas a la BBDD.	5	5	2	4	5	20-Muy alto	Política y gestión de perfiles con privilegios asignados por la naturaleza de sus funciones; restricciones a la generación de copias, modificación, eliminación, entre otros.	En principio no, pero se considera que reduce a 3. Impacto residual=3	Sí. Probabilidad residual =3	9-Medio
Análisis de la medida en lo particular Esta medida pertenece a la categoría de control de accesos, que busca prevenir accesos no autorizados a la información en activos físicos como en activos electrónicos. La gestión de perfiles y privilegios es una medida preventiva. Asimismo, la política que se haga al respecto es una medida disuasoria además de preventiva, toda vez que la persona que intervenga en el tratamiento o en el activo, sabrá que debe cumplir con la política y hay consecuencias de no hacerlo, cuestión que incide en la probabilidad del escenario del riesgo. Conforme a la categorización de la Ley General la gestión de perfiles y privilegios en un entorno digital es una medida de seguridad técnica; por otra parte, la política que se realice sobre dicha gestión es una medida administrativa y ambas van a proteger lo mismo y se complementan. Es importante reiterar que una política no funcionará por si misma si no se comunica y no se capacita al personal que la operará. **¿Reduce impacto?** En principio no reduce el impacto puesto que, aunque se controlen las copias generadas, las personas autorizadas para obtenerlas pueden hacer un mal tratamiento, y el impacto en las personas titulares puede ser grave. Sin embargo, es posible que se reduzca el riesgo de pérdida de confidencialidad en tanto que se limita a las personas que tratan esos datos que, con esta medida, al tener mayor control y trazabilidad de la información y de las personas, disminuya el impacto por cuanto a las acciones reactivas que deriven de ser descubierta la vulneración.										

ACTIVO: RENMS-BBDD										
Escenario de vulneración	**Impacto**									
	C	**I**	**D**	**Impacto total**	**Prob**	**Riesgo inherente**	**Control implementado**	**¿Reduce impacto?**	**¿Reduce probabilidad?**	**Riesgo residual**
Supongamos que la confidencialidad disminuye a 4, al igual que la integridad porque su afectación es más controlable y la disponibilidad se mantiene en 1, (4+4+1=9/3=3) por lo que el impacto residual es 3. **¿Reduce probabilidad?** Sí. Esta medida al ser preventiva y disuasoria puede incidir más en la probabilidad, aunque al depender de la voluntad de personas, el escenario no es del todo controlable, sin embargo, el activo pasa a estar configurado para evitar copias no supervisadas de los datos personales, permitiendo tener la trazabilidad de los datos; aunque el escenario podría seguir ocurriendo incluso si se generan copias controladamente por terceros autorizados. En ese sentido se considera viable reducir la probabilidad a 3.										
4. Acceso no autorizado, uso indebido de los datos personales, porque no se cuentan con protocolos de intercambio seguro de información.	5	5	1	4	5	20-Muy alto	Se deberán implementar controles de cifrado en el intercambio de información a fin de generar un canal de comunicación seguro entre los usuarios y el aplicativo.	Si. Impacto residual=2.3=2	En principio el control no reduce probabilidad de la amenaza, pero sí de la materialización del escenario. Probabilidad residual=4	8-Medio
Análisis de la medida en lo particular Esta medida pertenece a la categoría de criptografía y seguridad en las comunicaciones, que busca prevenir la intercepción de la información en reposo o en tránsito, en este caso se trata de un control para información en tránsito, ya que se cifra a fin de que en el caso de que un tercero no autorizado la intervenga no pueda ver la información. En ese sentido es una medida preventiva, que incide en el impacto, ya que, aunque se intente intervenir o acceder a la información en tránsito, esta no estará accesible o entendible para el tercero y por lo tanto el riesgo no se materializará, salvo que pueda descifrarla. Conforme a la categorización de la Ley General la encriptación o cifrado es una medida de seguridad técnica. **¿Reduce impacto?** Sí. Esta medida incide directamente en las propiedades de confidencialidad e integridad. Por lo que reduce a 3 y la disponibilidad se mantiene en 1 (3+3+1=7/3=2.3). **¿Reduce probabilidad?** No, en principio esta medida previene el impacto, no así la probabilidad, puesto que depende de la voluntad de terceras personas, sin embargo, es menos probable que se materialice una vulneración, aunque, persiste la probabilidad de sufrir ataques como "man in the middle" u hombre en medio y sus variantes, donde un atacante se infiltra entre el sistema de la víctima y un recurso de Internet utilizado por la víctima. En ese sentido se decide reducir a 4.										

ACTIVO: RENMS-BBDD										
Escenario de vulneración	**Impacto**									
	C	**I**	**D**	**Impacto total**	**Prob**	**Riesgo inherente**	**Control implementado**	**¿Reduce impacto?**	**¿Reduce probabilidad?**	**Riesgo residual**
5. Pérdida de disponibilidad en el aplicativo por una gran cantidad de solicitudes legítimas, y no se cuenta con un servidor o una aplicación redundante.	1	1	2	1	4	4-Bajo	Se deberá implementar un servicio que brinde redundancia para atender una gran cantidad de solicitudes de servicio sin quedar fuera de línea.	Si. Impacto residual =1	En principio no disminuye la probabilidad de la amenaza, pero disminuye la probabilidad de materialización Probabilidad residual=3	3-Bajo
Análisis de la medida en lo particular Esta medida pertenece a la categoría de tecnología- redundancia de recursos, que busca prevenir la falta de disponibilidad de la información. Es, por lo tanto, una medida preventiva, y en este caso incide en el impacto, toda vez que al establecer un sistema redundante se espera que el sistema siga en operación y disponible, sin afectar o traer consecuencias a los servicios. Conforme a la categorización de la Ley General es una medida de seguridad técnica. **¿Reduce impacto?** Sí, la confidencialidad e integridad se mantienen en 1, la disponibilidad disminuye a 1, ya que no es posible reducirla más, aunque el resultado de impacto total sigue siendo 1. Ahora bien, hasta no conocer el tráfico real de solicitudes no se tendría la certeza del comportamiento de la medida implementada, pero es posible con esta medida, mantener la operabilidad. **¿Reduce probabilidad?** No reduce el origen de la amenaza, puesto que las solicitudes se seguirán realizando, toda vez que la gente requiere realizar el registro, sin embargo, reduce la probabilidad de la falta de disponibilidad. Por lo que en este caso se estima pertinente reducirla a 3.									
6. Posible ataque DoS, que puede ocasionar una falta de disponibilidad del aplicativo por la cantidad de solicitudes de conexión malintencionadas.	1	1	5	2	3	6-Medio	Se deberán implementar controles de monitoreo de tráfico a fin de identificar solicitudes legitimas de uso que permite el aplicativo de manera simultánea a fin de configurar bloqueos a conexiones malintencionadas.	Sí. Impacto residual= 2.	En principio no disminuye la probabilidad de la amenaza, pero sí de la materialización del riesgo. Probabilidad residual=2	4- Bajo

ACTIVO: RENMS-BBDD										
Escenario de vulneración	Impacto				Prob	Riesgo inherente	Control implementado	¿Reduce impacto?	¿Reduce probabilidad?	Riesgo residual
	C	I	D	Impacto total						
Análisis de la medida en lo particular Esta medida pertenece a la categoría de Tecnología- seguimiento de actividades, que busca monitorear la red y bloquear las solicitudes malintencionadas, con ello, es posible prevenir la falta de disponibilidad de la información. Es, por lo tanto, una medida de monitoreo y correctiva, e incide en el impacto al bloquear las conexiones malintencionadas y la probabilidad de materialización del escenario al monitorear la red, toda vez que saltan avisos para desplegar otras medidas reactivas complementarias, en este caso, evitar la falta de disponibilidad del registro. Conforme a la categorización de la Ley General es una medida de seguridad técnica. **¿Reduce impacto?** Si, puesto que bloquea las conexiones mal intencionadas, y con ello se detendría la materialización del escenario, aunque es posible que no sea suficiente. En ese sentido la confidencialidad e integridad se mantienen en 1, y la disponibilidad se reduce a 3, por lo que 1+1+3=5/3=1.6=2; en este caso, a pesar de que se reduzca el valor de afectación de la disponibilidad, no reduce el impacto total.										
¿Reduce la probabilidad? En principio no incide en la probabilidad de la amenaza, ya que esta depende de terceros (los atacantes que pretenden dejar indisponible el servicio mediante un ataque de DoS), sin embargo, si incide en la materialización del escenario, en tanto que monitorea la red y es posible que se desplieguen otras medidas para reducir la posibilidad de que se materialice el riesgo. Por ello se considera viable reducir la probabilidad a 2.										

Tabla 21. Obtención del riesgo residual (primera iteración con medidas implementadas)
Autoría propia

En el ejemplo se pueden observar seis escenarios de vulneración, cada uno con solo una medida de seguridad, para el mismo activo. Medidas que, en este caso, se están considerando como ya implementadas en el sujeto obligado.

Respecto del activo y los escenarios es importante observar que, en algunos casos, el escenario de vulneración describe una afectación directa a otro activo (por ejemplo, los posibles ataques de DoS a los servidores institucionales), pero que, indirectamente afecta al activo analizado (el RENMS BBDD), esto es porque existirán escenarios de vulneración que, al afectar algunos activos críticos, indirectamente afectarían a otros que dependen de ellos.[59]

Asimismo, es posible observar cómo la medida de seguridad prevista disminuye el nivel de riesgo de cada escenario, sin embargo, en dos casos no los reduce a un riesgo bajo, o muy bajo, es decir, un riesgo aceptable.

El sujeto obligado podría decidir aceptar un riesgo con un nivel no aceptable de acuerdo a su metodología, en casos donde esté imposibilitado de implementar más medidas, en esos supuestos, es recomendable que se firme un acta por el

59 La Metodología Magerit (Libro I) explica muy bien esta situación ya que la descripción para el inventario de activos la hace mediante árbol de dependencias, donde considera importante el mapeo de todos los activos en forma de árbol genealógico, donde hay activos que denomina padres e hijos.

Comité de Transparencia, los titulares de la unidad administrativa o los propietarios del tratamiento, así como, de ser posible, de alguna persona integrante de Órganos Directivos o de Gobierno, a efecto de que quede claro el motivo de la falta de atención a determinados riesgos, así como la cadena de rendición de cuentas, en el entendido de que es parte del principio de responsabilidad que debe cumplir el responsable del tratamiento: *destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales*[60], políticas y programas que soportan el deber de seguridad.

Debe quedar claro que, el hecho de aceptar un riesgo de un nivel mayor al aceptable, y en caso de vulneración, puede traer consecuencias para el responsable del tratamiento, por no cumplir con los deberes de seguridad y el principio de responsabilidad.

Ahora bien, una vez realizada la primera iteración, y teniendo la fotografía actual de las medidas de seguridad implementadas, es importante medir su nivel de madurez.

Análisis del nivel de madurez

Se debe analizar el nivel de madurez de las medidas de seguridad, esto se refiere a que se debe evaluar qué tan correctamente implementadas están las medidas de seguridad, y si son medibles; en este primer ejercicio podremos valorar el grado de implementación y comenzar a ver los indicadores para la evaluación de su efectividad.

De acuerdo con la metodología MAGERIT, se considera que una medida de seguridad tiene una eficacia del 0% cuando es inexistente y un 100% aquellas que están implantadas, que son idóneas, son medibles, existen procedimientos claros de uso normal y en caso de incidencias, los usuarios están formados y concienciados a efectos de responder y reactivarlas o ponerlas en operación.

Para medir los aspectos organizativos, MAGERIT propone la siguiente escala de madurez de los controles:

Porcentaje de implementación	Nivel		Criterio
0%	L0	Inexistente	Inexistente
	L1	Inicial/ad hoc	Se realiza cuando se detecta un problema, no existe previsión es una medida reactiva
	L2	Repetible pero intuitivo	Hay una persona que, sin ser responsable, la realiza de forma preventiva y constante de acuerdo con su criterio, tampoco está documentada.

60 Artículo 30, fracción I de la LGPDPPSO.

	L3	Proceso definido	Está documentada, tiene un responsable y está implementada
	L4	Gestionado y medible	Además de estar documentada y funcionando, es medible
100%	L5	Optimizado	Además de ser medible, está automatizada, y pueden saltar avisos cuando hay problemas en su implementación

Tabla 22. Ejemplo de escala de madurez para las medidas de seguridad

De acuerdo con la escala anterior, se propone que el sujeto obligado realice una tabla con los activos, el escenario de vulneración, el valor del riesgo inherente y la columna de control o medida de seguridad ya implementada, el nivel de madurez de la medida, y es deseable que se identifique el responsable de la medida, así como la evidencia del cumplimiento del control.

Ejemplo:

ACTIVO: RENMS BBDD					
Escenario de vulneración	**Riesgo inherente**	**Control implementado**	**Riesgo residual**	**Nivel de madurez**	**Persona responsable de implementarla u operarla**
3. Accesos no autorizados por terceros e indebido tratamiento de datos personales por personas autorizadas; ello, por no contar con una política de gestión de perfiles y privilegios, y no controlar las copias generadas a la BBDD.	20-Muy alto	Política y gestión de perfiles con privilegios asignados por la naturaleza de sus funciones; restricciones a la generación de copias, modificación, eliminación, entre otros.	9 - Medio No aceptable	L3-Proceso definido. La medida está documentada.	
Análisis de la madurez de la medida de seguridad: En este caso, es posible analizar una medida en dos etapas, la primera la política de gestión de perfiles y privilegios, y segunda la operación misma de la medida. Esto se propone así, ya que la propia Ley General establece como medidas de seguridad administrativas todas las políticas, y a la gestión de perfiles y privilegios como medida de seguridad técnica, en ese sentido, podemos ver dos medidas conforme a la Ley General, y estas se complementan. Es por eso que, conforme a la propuesta de niveles de madurez, se le otorga un nivel 3, ya que la medida está documentada en una política, y supuestamente hay un responsable de operarla. En caso, por ejemplo, de que la medida se operara de facto, por mera intuición del custodio o administrador del sistema, se le tendría que valorar con un nivel 2 repetible pero intuitivo.					

Tabla 23. Ejemplo del análisis del nivel de madurez de una medida de seguridad

Posterior a la primera iteración y la evaluación de la madurez de las medidas actuales, es posible buscar las medidas idóneas y oportunas para los riesgos residuales prioritarios, es decir los que han tenido los niveles más altos. Por orden de prioridad el ideal es implementar medidas para los riesgos muy altos, posteriormente los altos, después los medios y finalmente los bajos, los cuales se pueden mantener así mientras estén monitoreados. En cuanto a los casos prácticos de ejemplo, los riesgos prioritarios son los escenarios de vulneración 3 y 4 que tienen un riesgo medio.

Ahora bien, lo anterior no obsta para que se implementen todas las medidas de seguridad que sea posible del catálogo seleccionado, de hecho, muchas de las medidas aplicables a un riesgo en particular se aplican en lo general; por ejemplo, en caso de establecerse una política de gestión de perfiles y privilegios, esta debe ser general para todos los sistemas de información, sin embargo, cuando se opere, aplicará directamente para el activo analizado y en riesgo, se atiende el riesgo particular.

Una vez que se ha decidido qué medidas de seguridad faltan (tabla o declaración de aplicabilidad) y de esas cuáles son prioritarios para atender los riesgos más altos es recomendable realizar otra iteración del análisis de riesgos residual, donde se valore en prospectiva, cuanto se espera que reduzca el riesgo.

Ejemplo:

<table>
<tr><th colspan="6">ESCENARIO DE RIESGO</th></tr>
<tr><th>Escenario de vulneración</th><th>Riesgo inherente</th><th>Control implementado</th><th>Riesgo residual</th><th>Madurez</th><th>Persona responsable de operarla</th></tr>
<tr><td rowspan="2">4. Acceso no autorizado, uso indebido de los datos personales, porque no se cuentan con protocolos de intercambio seguro de información.</td><td rowspan="2">20-Muy alto</td><td rowspan="2">Se deberán implementar controles de cifrado en el intercambio de información a fin de generar un canal de comunicación seguro entre los usuarios y el aplicativo.</td><td>1era Iteración
<table><tr><th>Impacto</th><th>Probabilidad</th></tr><tr><td>C=3
I=3
D=1
Impacto residual =2</td><td>Probabilidad residual=4</td></tr></table>Riesgo residual= 8-Medio</td><td rowspan="2">L3</td><td rowspan="2"></td></tr>
</table>

<table>
<tr><th></th><th>Controles adicionales para implementar</th><th>Riesgo residual</th><th>Madurez</th><th>Perso-na(s) respon-sables de imple-mentar y operar</th></tr>
<tr><td></td><td>1. Cifrado de información en reposo.</td><td><table><tr><th>Impacto</th><th>Probabilidad</th></tr><tr><td>C=2
I=2
D=1
Impacto residual= 1.6=2</td><td>Probabili-dad resi-dual= 3</td></tr></table>Riego residual= 6-Medio (Riesgo residual, se-gunda iteración (pros-pectiva[61]))</td><td>L0</td><td></td></tr>
<tr><td colspan="5">Esta medida de seguridad es técnica y preventiva e incide en el impacto principalmente, ya que, si terceros no autorizados quieren acceder a la información, no podrán visualizarla ya que estará cifrado el canal de comunicación, pero también cuando reposa en servidor.</td></tr>
<tr><td></td><td>2. Seguridad en las comunica-ciones- Política de restricción de mensajería: Se establecen restricciones para el envío y recepción de información por correo electró-nico y mensaje-ría instantánea; limitación de la utilización de redes sociales en equipos del sujeto obligado.</td><td><table><tr><th>Impacto</th><th>Probabilidad</th></tr><tr><td>C=2
I=2
D=1
Impacto residual= 1.6=2</td><td>Probabili-dad resi-dual= 2</td></tr></table>Riego residual=4-Bajo (Riesgo residual, segunda itera-ción-prospectiva)</td><td>L0</td><td></td></tr>
<tr><td colspan="5">Esta medida de seguridad es administrativa y preventiva e incide tanto en la probabilidad, puesto que es posible que reduzca la posibilidad de que terceros no autorizados accedan o intervengan en la comunicación que se comparta puesto que se limitan las vías inseguras.</td></tr>
</table>

Tabla 24. Ejemplo de análisis prospectivo del riesgo residual con las medidas seleccionadas para implementarse Autoría propia

61 Esta segunda iteración del análisis de riesgo residual con medidas de seguridad que se van a implementar es meramente prospectiva, es decir, se valora lo esperado, previo a la implementación y se comprobará hasta que se ponga en marcha la medida.

Hasta este momento, tenemos en lo que respecta al tratamiento del riesgo, el análisis de brecha con la identificación de las medidas existentes, las medidas faltantes y las que se pueden mejorar, esto a través de la guía de algún o algunos catálogos de medidas de seguridad, una vez esto, se debieron especificar las medidas de seguridad a los riesgos particulares, en este caso los prioritarios. Asimismo, para saber la efectividad de las medidas actuales, se realizó la primera iteración del análisis de riesgos residual, donde se analiza la medida en particular y el nivel de implementación (nivel de madurez de las medidas actuales), obteniendo el panorama objetivo del riesgo actual en la entidad, y finalmente, de las medidas seleccionadas para implementar (faltantes), un estimado prospectivo del riesgo residual.

Una vez que hemos decidido todas las medidas de seguridad faltantes de los riesgos prioritarios, entonces podemos pasar al último paso del tratamiento del riesgo que es la planeación de actividades para la implementación.

Plan de trabajo

El plan de trabajo es la hoja de ruta para la implementación de las medidas de seguridad o controles que se seleccionaron en el análisis de brecha. Asimismo, además de la implementación se buscará madurar la medida implementada.

En este paso se deben establecer las actividades particulares a realizar para implementar los controles, asimismo, se definirán plazos y recursos a utilizar, e incluso el responsable de realizar cada actividad, así como un encargado de revisar la operación.

Al respecto la Ley General y los Lineamientos Generales señalan:

Artículo 33 de la Ley General

"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

(...)

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;"

(...)

Artículo 62 de los Lineamientos Generales

"De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes."

Por lo que, para el plan de trabajo es posible seguir utilizando el formato propuesto para el análisis de riesgos y de brecha, y agregar si el control es prioritario, las actividades o proyectos a realizar para la implementación del control, los plazos límites, los responsables de operarlas, los recursos necesarios, así como cuándo y quién revisará la operación del control.

Ejemplo:

Escenarios de vulneración	**Control(es) de seguridad**	**Estatus**	**RR**	**Prioridad**	**NM**
Se identifica que los protocolos de transmisión de datos entre el usuario y el servidor no seguros son más vulnerables.	Se deberán implementar controles de cifrado en el intercambio de información a fin de generar un canal de comunicación seguro entre los usuarios y el aplicativo.	Por implementar	4-Alto	Alta	L3-
Actividades para implementación o mejorar las MS / Fecha de operación				**Encargado de operación/ participantes**	**Recursos**
Integración de certificados SSL Implementación		Inicio: 16/09/2023 Término-18/09/2023		Operación: Titular DGTI Participantes: directores de área DGTI y personal operativo.	Costo de certificados SSL

RR= riesgo residual
NM= Nivel de madurez de la medida de seguridad

Tabla 25. Ejemplo de plan de trabajo
Autoría propia

Aunado a lo anterior, es recomendable establecer además revisiones periódicas de cada control, así como la persona encargada de dicha revisión, esto será muy importante para la siguiente fase de implementación y operación, en tanto que debe ser parte de la operación continua del sistema de gestión. De igual forma deben trabajarse indicadores y métodos para evaluar la eficacia de las medidas.

Como puede observarse, la gestión del riesgo involucra el análisis de riesgos, el tratamiento del riesgo a través del análisis de brecha, y finalmente el plan de trabajo con el que se plantean de forma sistematizada las actividades para la puesta en operación de los controles de seguridad.

La gestión del riesgo será el soporte para la toma de decisiones estratégicas para tratar el riesgo, donde se busca mantener el riesgo en un nivel aceptable, así como un apoyo en la definición y asignación efectiva de recursos, justificar esfuerzos en tiempo, recursos humanos y financieros, por lo que es uno de los pilares de los sistemas de gestión de seguridad de la información.

Fase 2. Implementar y operar el Sistema de Gestión de Seguridad de Datos Personales

Implementar el sistema de gestión significa introducir o integrar todos los procesos que de este derivan en los procesos de la entidad, en esta fase se debe implementar todo lo trabajado durante la Fase 1 de planeación, es decir se deberán incorporar y operar las políticas, procesos, procedimientos y controles del SGSDP y las medidas de seguridad que hayan resultado aplicables según el análisis de brecha y se pondrá en marcha el plan de trabajo.

Obtención de documentación de soporte

Todas las fases y pasos del sistema de gestión deben estar documentados, a fin de poder observar, demostrar y evaluar la operación del sistema de gestión y el cumplimiento de los objetivos de seguridad impuestos por el sujeto obligado, será fundamental para evaluar el progreso de la implementación y operación del propio sistema y por lo tanto para la mejora continua. Asimismo, para efectos del monitoreo y revisión, por ejemplo, en los procesos de auditoría, se solicitará toda la documentación, registros y evidencias.

Control de cambios

De igual manera deberá idearse como mantener documentado y el histórico de los cambios que se realicen en la operación del sistema de gestión, o cualquier incidente que lo altere, particularmente en:

- Cambios en procesos o procedimientos
- Eventos o incidentes de seguridad de la información que afecte a datos personales
- Auditorías y sus resultados
- Cambios que deriven de las reuniones periódicas de revisión al sistema de gestión

Capacitación y concienciación

La capacitación es fundamental para la seguridad de los datos personales, de acuerdo con la Ley General, la capacitación es una medida de seguridad administrativa

Artículo 2 de la Ley General:
"Para los efectos de la presente Ley se entenderá por:
(...)
XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;
(..)"

Por ello, 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. En ese sentido es fundamental implementar capacitación a personal interno y externo al sujeto obligado, de acuerdo con los roles y responsabilidades establecidos en el paso 4, funciones y obligaciones.

El responsable 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.

En ese sentido, es importante diferenciar la sensibilización o concienciación, de la capacitación. La primera es la formación básica en materia de protección de datos personales y seguridad, respecto a los contenidos y conceptos de la Ley General, sus principios, deberes y obligaciones que debe ser impartida a todo el personal de la entidad, y que busca que la cultura de la seguridad de los datos personales permee en la propia organización, y por otra parte la capacitación, donde se deben establecer niveles de especialización ya que hay personal que requerirá un nivel de capacitación técnica y especializada atendiendo a las funciones que desempeñan y en las que se encuentre inmerso el tratamiento de datos personales, por ejemplo, un servidor público que opera un software que contiene una gran base con datos personales sensibles, requiere de una capacitación más técnica y especializada de aquél que cuya función sea recabar datos personales en un formato físico y que no contenga datos personales sensibles, aunque es importante que todos estén sensibilizados en materia de protección de datos personales a efecto de que comprenden la razón de las funciones de seguridad y por qué deben proteger los datos personales. Por ello es indispensable identificar cuál es su contribución y cuáles son sus funciones para cumplir con los objetivos de seguridad planteados en el SGSDP del sujeto obligado.

Ahora bien, para asegurar la capacitación dentro del sujeto obligado, la Ley General y los Lineamientos establecen como deber para el responsable:

Artículo 30 de la Ley General:
"Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de Responsabilidad, establecido en la presente Ley están, al menos, los siguientes:
I. (...)
II.
III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
(...)"
tección de datos personales;
(..)"

Artículo 48 de los Lineamientos Generales:
"Capacitación.
(Con relación al artículo 30, fracción III de la Ley General, el responsable deberá establecer anualmente un programa de capacitación y actualización en materia de protección de datos personales dirigidos a su personal y a encargados, el cual deberá ser aprobado, coordinado y supervisado por su Comité de Transparencia.

Artículo 33 de la Ley General:
"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:
(...)
VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales."

Artículo 64 de los Lineamientos Generales:
"Capacitación.
Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.
En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;

> **III.** Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
> **IV.** Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad."

El programa de capacitación debe atender todos los requerimientos de los artículos antes citados, en primer lugar, el artículo 30, fracción III establece que para el cumplimiento del principio de responsabilidad el sujeto obligado debe poner en marcha un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales, este programa, de acuerdo con el artículo 48 de los Lineamientos Generales, debe realizarse anualmente y ser aprobado, coordinado y supervisado por el Comité de Transparencia.

Por su parte el artículo 33 establece que el responsable debe diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades que desempeñen en el tratamiento de los datos personales.

El artículo 64 de los Lineamientos es aún más específico y establece la obligación de implementar programas a corto, mediano y largo plazo, además de considerar los niveles en la capacitación de acuerdo con los roles y responsabilidades, y señala que se deben tomar en cuenta elementos como:

- **a)** Requerimientos y actualizaciones al contexto del SGSDP, considerando principalmente; las mejoras a este, modificaciones en la operación de las medidas de seguridad, la gestión de incidentes y vulneraciones de seguridad.
- **b)** La legislación en protección de datos personales y cuestiones de autorregulación y mejores prácticas relacionadas al tratamiento de datos aplicables al sujeto obligado;
- **c)** Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, por ejemplo, incumplimientos a las políticas, programas y procedimientos institucionales en materia de protección de datos personales o de seguridad.
- **d)** Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad.

Finalmente, se recomienda 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 el sujeto obligado, y mantener un registro de los programas seguidos por cada empleado, así como de sus habilidades, experiencia y calificaciones.

Es importante que el responsable documente y tome evidencias de las capacitaciones que se imparten, a efectos de demostrar el cumplimiento en los medios de revisión, como pueden ser auditorías internas, externas o voluntarias y para efectos de la evaluación de la capacitación como medida de seguridad administrativa. Es importante señalar que la comprobación de recursos, la capacitación, y el control operacional a través de la documentación de todas las acciones para la implementación del sistema de gestión no deben verse como pasos a seguir exclusivamente en esta fase del ciclo, puesto que como se señaló al inicio existen procesos dentro del sistema de gestión que deben implementarse a lo largo de todo el ciclo de mejora. Es decir, la capacitación, por ejemplo, no puede desarrollarse solo en la fase de implementación, quizá se realizarán acciones desde la planeación, posteriormente en la gestión del riesgo podrían derivar riesgos por la falta de ésta, y se deba implementar como medida de seguridad en el plan de trabajo, ya que la capacitación es una medida de seguridad administrativa. Asimismo, la documentación del sistema a través de registros y evidencias debe realizarse desde la planeación y no solo durante la implementación como tal.

En conclusión, los recursos, la sensibilización y capacitación, y el control operacional, son el soporte de todo el sistema, son procesos transversales que inciden en todo el ciclo de mejora.

Paso 6. Implementación del Plan de Trabajo

La implementación de las medidas de seguridad es poner en práctica el plan de trabajo elaborado en el último paso de la fase de planeación, en la gestión del riesgo. Es decir, se deberán poner en operación las medidas de seguridad faltantes y se deben fortalecer las ya implementadas a fin de mejorar su madurez, en los tiempos y con los recursos planeados, aunque siempre es posible modificar dicha planeación, de acuerdo al contexto del sujeto obligado.

Durante la implementación de las medidas de seguridad se debe considerar también, la toma de registros y evidencias para efectos de contar con el histórico de su operación, de igual forma, como se señaló en el paso 5.2. en el plan de trabajo, deberá establecerse un encargado de revisar que la medida en particular se opere continuamente, estableciendo revisiones periódicas, y buscar el fortalecimiento del nivel de madurez de las medidas de seguridad. En este punto debe comprenderse que no solo debe velarse por el cumplimiento de la medida como fue planeada, es decir a nivel de operación sino también valorar su eficacia, para lo que deberán irse consolidando indicadores como se verá en la siguiente fase de monitoreo y revisión.

Fase 3. Monitorear y revisar el Sistema de Gestión de Seguridad de Datos Personales

En esta fase, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se hayan logrado los objetivos de seguridad planteados y la mejora esperada.

Para ello, la Ley General y los Lineamientos establecen:

33 de la Ley General

"Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

(...)

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

(...)"

Artículo 63 de los Lineamientos Generales

"Monitoreo y supervisión periódica de las medidas de seguridad implementadas al Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."

En ese sentido, la Ley General refiere al monitoreo particular de las medidas de seguridad implementadas, así como a las amenazas y vulneraciones a las que están sujetas los datos personales, así como los activos de información que contienen datos personales y los factores del riesgo.

El artículo 63 de los Lineamientos Generales por su parte, incorpora la medición de los resultados de las políticas, planes, procesos, etcétera, con el fin de verificar que estos estén siendo eficaces en el cumplimiento de los objetivos de seguridad planteados para implementar las mejoras oportunas; asimismo, señala que para poder evaluar las medidas es necesario analizar los nuevos activos del sujeto obligado, sus modificaciones, nuevas amenazas y vulnerabilidades no estudiadas con antelación, nuevas amenazas que exploten viejas vulnerabilidades no analizadas, el cambio en el impacto o en alguno de los factores del riesgo, que cambien el nivel de riesgo, a uno no aceptable, es decir, en la medida en la que analicemos si el riesgo disminuye o nos acercamos al nivel de riesgo aceptable, podremos observar si las medidas implementadas están siendo útiles.

Finalmente, el último párrafo establece que el responsable debe contar con un programa de auditoría interno y/o externo para monitorear y revisar la eficacia del propio sistema de gestión, lo cual es de suma relevancia, ya que en un sistema de gestión no solo deben monitorearse las medidas de seguridad y los factores del riesgo, sino el sistema en sí, desde los planteamientos de los objetivos, contexto, alcance, los criterios, la metodología para la gestión del riesgo, etcétera.

Ahora bien, para efectos de un cumplimiento idóneo del deber de seguridad en lo que respecta al SGSDP, se debe cumplir también con el principio de responsabilidad establecido en el artículo 30, fracciones V y VI de la Ley General, el cual impone obligaciones adicionales respecto al monitoreo y vigilancia o supervisión y vigilancia, en particular de las políticas y programas de gestión y tratamiento de datos personales y de seguridad, que al ser estos medidas de seguridad administrativas, inciden en el SGSDP. Al respecto la Ley señala:

Artículo 30 de la Ley General
"Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:
(...)
IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
(...)"

Artículo 49 de los Lineamientos Generales
"Sistemas de supervisión y vigilancia
Artículo 49. Con relación al artículo 30, fracciones IV y V de la Ley General, por regla general, el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización previa al plazo establecido en el presente artículo."

En ese sentido, las acciones planificadas para el monitoreo y revisión del sistema de gestión deberán estar contempladas en el sistema de supervisión y vigilancia a que refiere el artículo 49 de los Lineamientos Generales, y las revisiones de las políticas y programas deberá entenderse en conjunto o en armonía con la revisión del cumplimiento de las medidas de seguridad de manera continua dentro del sujeto obligado conforme a lo establecido en la implementación y operación del sistema de gestión; es decir, el monitoreo y revisión implica múltiples actividades que deben estar planificadas en un sistema de supervisión y vigilancia en el que se consideren:

- Revisión de los factores del riesgo
- Evaluación de la eficacia de las medidas de seguridad: esto implica todas las medidas, tanto físicas, técnicas como administrativas, recordando que dentro de esta últimas se encuentran las políticas y programas de seguridad. Esta evaluación debe realizarse mediante métricas e indicadores.
- Planes de auditoría internas y/o externas a las medidas de seguridad.
- Planes de auditoría internas y/o externas al SGSDP.
- Revisiones por el Comité de Transparencia-Directivos del Sujeto Obligado

Paso 7. Revisiones de los factores del riesgo-iteración de la gestión del 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 del sujeto obligado y así mantener una visión general de la imagen del riesgo.

En ese sentido, deberán realizarse iteraciones periódicas de la gestión del riesgo expuesto en el paso 5, es decir, debe volver a realizarse la gestión del riesgo, identificando lo que señala el artículo 63 de los Lineamientos Generales, incorporar los nuevos activos que se integren al sujeto obligado, sus vulnerabilidades, las amenazas, y los nuevos escenarios de vulneración que puedan surgir, así como la probabilidad de que se materialicen y el impacto en la entidad y en los titulares de los datos personales.

Dichas iteraciones del proceso de la gestión del riesgo deben realizarse continuamente, pueden programarse en plazos previamente establecidos, pero también es importante realizarlas cuando existan cambios en la entidad que afecten los tratamientos de los datos personales, como cuando se materialice alguna vulneración a la seguridad, cuando se migren activos a nuevas tecnologías y cuando existan modificaciones a los tratamientos de datos personales.

Paso 8. Evaluación de la eficacia de las medidas de seguridad

En el paso 6 se indicó que se debe revisar el cumplimiento continuo de las medidas de seguridad a un nivel de operación, sin embargo, en este paso se trata de medir la eficacia de la medida. En ese sentido, en el paso 5.2. particularmente en el plan de trabajo, se señaló también, que las medidas de seguridad deben contar con un método e indicadores a fin de evaluar su eficacia respecto al cumplimiento de los objetivos de seguridad planteados, a fin de identificar los ajustes que se requieren para mejorar su efectividad.

Es en este paso las medidas de seguridad, incluyendo las políticas de seguridad, deben ser evaluadas a través de dichos indicadores y métricas.

Para establecer los indicadores será importante preguntarse ¿cuál es el motivo u objetivo de haber impuesto la medida de seguridad? y analizar si realmente el riesgo que está combatiendo esa media disminuyó. Se debe tener claro que "*la efectividad de los controles o medidas de seguridad debe estar asociada con el nivel de cumplimiento con respecto del objetivo que dio origen al control y no con qué tantas veces se realicen las actividades*"[62] que involucra su operación (esto es parte de la operación de las medidas de seguridad, paso 8).

Para la creación de la métrica e indicadores de desempeño debe identificarse lo que se espera de cada control en función de los objetivos para los que fue implementado, establecer métricas de cumplimiento, "(…) *establecer mecanismos de medición que permitan monitorear de forma continua y consistente los controles, establecer indicadores clave del desempeño (KPI), relacionando distintas métricas que brinden información para la toma de decisiones, y establecer metas sobre el cumplimiento de los KPI establecidos* (…)"[63].

Como se observa al contar con estas métricas para valorar la eficacia de las medidas, se estaría cumpliendo con un nivel de madurez L-4 Gestionado y medible (véase Paso 5.2. análisis de brecha), que es el mínimo recomendado para que se considere que una medida de seguridad realmente está funcionando y está siendo evaluada constantemente, toda vez que es una prueba de que es posible mejorar el sistema de gestión.

62 Corona Fraga, Pablo. Guía práctica para la gestión de riesgos en la era de la ciberseguridad. (julio 2019) Primera edición. México. Thomson Reuters. P.102.

63 Ibidem. p.103.

Debe considerarse, que en muchos casos la efectividad real de las medidas la sabremos hasta que exista una vulneración de seguridad a los datos personales, o bien se realicen ejercicios de simulación de vulneraciones, estos últimos recomendables, y que en ambos casos deben servir para aprender, modificar y corregir, es decir para la mejora continua.

Paso 9. Auditorías internas y externas

Es importante distinguir la diferencia entre la evaluación de las medidas de seguridad, que pueden realizarse a diario en el sujeto obligado, de las auditorías al SGSDP, ya que en las primeras se va a enfocar en el análisis de la eficacia de las medidas como resultado de una gestión del riesgo, y las auditorías a que refiere el último párrafo del artículo 63 de los Lineamientos Generales, es una revisión del Sistema, lo que incluye su planeación, implementación, operación, revisión y actualización, es decir toda la operación para el alcance estipulado, esto es, el tratamiento o los tratamientos de datos personales que se van auditar que estén incorporados al SGSDP.

Como se señaló, de acuerdo con el último párrafo del artículo 63 de los Lineamientos Generales, es obligatorio para el responsable del tratamiento contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión; por ello, se deberán planear las auditorías internas y/o externas correspondientes, siendo recomendable realizar ambas, es decir, auditorías tanto internas, como externas.

Las auditorías internas deben realizarse en intervalos planificados para proporcionar información sobre si el SGSDP cumple con los requisitos propios del sujeto obligado. El reto que se encuentra en este tipo de auditorías es la independencia de los auditores, ya que, al ser interna, serán personas que laboren dentro de la propia entidad, y pueden ser parciales en sus conclusiones, sin embargo, se recomienda se realicen lo mejor posible, a efectos de que, si se busca una auditoría externa para efectos de una certificación o una auditoría voluntaria, la entidad pueda demostrar que el SGSDP está operando correctamente en búsqueda de la mejora continua.

Un programa de auditoria debería contemplar

- La frecuencia y las fechas previstas
- El alcance de la auditoría interna,
- Los métodos por los cuales se llevará a cabo la auditoría interna
- La asignación de responsabilidades para la planificación, la realización y la presentación de informes de los resultados de la auditoría interna.

Respecto al equipo auditor en auditorías internas, se recomienda designar por lo menos tres, aunque dependerá del tamaño del sujeto obligado; del equipo se recomienda que algunos desempeñen preferentemente puestos de mando para velar por su independencia en la medida de lo posible, y que puedan tener acer-

camiento con la alta dirección u Órganos Directivos o de Gobierno, asimismo, es importante que se considere a personas que pertenezcan a las unidades administrativas que realicen tratamientos de datos personales relevantes, incluso, de ser posible, una persona por unidad administrativa (siempre que sean unidades que realicen tratamientos u operen sistemas del tratamiento).

Además de las auditorías internas, es recomendable realizar auditorías externas para procesos y circunstancias especiales, por ejemplo, cuando el sujeto obligado desee unirse a un esquema de certificación.

En este caso, se deben establecer previamente los objetivos de la auditoría, el cual debe incluir el alcance e indicar explícitamente cualquier tratamiento de datos personales interno y externo al sujeto obligado, responsables, recursos, criterios a utilizar durante la auditoría, así como los procesos y/o áreas que serán auditadas.

Para la atención a la auditorías es recomendable que sea el Comité de Transparencia dentro del sujeto obligado quien coordine y las atienda en primera instancia, así como quien reciba los reportes, a fin de que gestione con los operadores, propietarios y custodios de los tratamientos y encargados de la operación del sistema de gestión la contestación a las observaciones y no conformidades correspondientes, lo que servirá también para coordinar la siguiente fase del sistema, de mejora del SGSDP.

Las auditorías pueden ofrecer al responsable, información detallada respecto a la efectividad del sistema de gestión, incluyendo la gestión del riesgo, sus resultados, y las evaluaciones de las medidas de seguridad.

Es recomendable realizar una auditoría después de la implementación de modificaciones mayores en el SGSDP o en los procesos críticos del sujeto obligado respecto al tratamiento de datos personales.

Auditorías voluntarias

Los sujetos obligados podrán someterse a auditorías voluntarias por parte del Instituto, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General y demás normativa que resulte aplicable. En ese sentido, es posible que la auditoría voluntaria conste de la revisión del sistema de gestión como deber de seguridad contenido en la Ley General, la auditoría es simplemente para verificar el cumplimiento de principios, deberes y obligaciones en materia de protección de datos personales.

Al respecto, la Ley General y los Lineamientos Generales contemplan respecto a las auditorías la figura de auditoría voluntaria:

Artículo 151 de la Ley General:
"Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los Organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan."

Artículo 218 de los Lineamientos Generales:
"Auditorías voluntarias
De conformidad con lo previsto en el artículo 151 de la Ley General, los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto, las cuales tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General y los presentes Lineamientos generales.

El Instituto, en su caso, podrá proponer la realización de auditorías programadas por sectores específicos conforme al programa de trabajo que sea aprobado para tal efecto."

Revisiones al sistema de gestión ante vulneraciones de seguridad

Además de las revisiones programadas ya sea a través de la planeación de iteraciones a la gestión del riesgo cada cierto tiempo, así como mediante auditorías y demás mecanismos que consten en el sistema de revisión y vigilancia, es necesario revisar el sistema de gestión cuando ocurra una vulneración de seguridad.

Una vulneración a la seguridad de los datos personales es, de acuerdo con la Ley General:

Artículo 38 de la Ley General:
"Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:
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".

Una vulneración a la seguridad es la materialización de un riesgo, es decir, que una amenaza vulnere un activo causando un impacto negativo en el sujeto obligado y en los titulares de los datos personales, se trata en general de la transgresión a una o algunas de las propiedades de la información: confidencialidad, integridad y/o disponibilidad.

El sujeto obligado tiene obligación de contar con un protocolo de actuación ante una vulneración de seguridad conforme al artículo 37 de la Ley General, en tanto que debe analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita. Aunado a esto, el responsable tiene obligación de informar sobre la vulneración a los titulares afectados, así como al Instituto.

Es importante observar que la Ley establece que debe implementarse en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad, lo que implica una revisión a la gestión del riesgo a efectos de valorar que medida no fue efectiva, o si se trató de alguna amenaza o vulnerabilidad no analizada, es de suma importancia comprender que todo lo que se realice en esa etapa debe estar documentado mediante registros y evidencias a efectos de 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.

Paso 10. Revisión por el Comité de Transparencia/Directivos

Es muy importante que la alta dirección del sujeto obligado esté involucrada en el proceso de implementación y en la operación del sistema de gestión, es por ello, que es recomendable establecer reuniones periódicas donde se evalúe la efectividad del sistema de gestión y se revise el progreso de las acciones requeridas para mejorarlo.

A las reuniones de revisión es importante que asistan personas con puestos de mando, que tengan intereses y aportación en el SGSDP, por ejemplo, propietarios de tratamientos y de activos que contienen datos personales, como Titulares de las unidades administrativas de Recursos Humanos, de Tecnologías de la información y Comunicaciones o similares, de la Dirección General de Administración, el Comité de Transparencia, entre otros.

Fase 4. Mejorar el Sistema de Gestión de Seguridad de Datos Personales

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 obtenidas a través del monitoreo, para lograr la mejora continua.

Paso 11. Mejora Continua

La mejora continua es lo que se busca en un sistema de gestión, en tanto que de la operación del sistema y su monitoreo y revisión se desprenderán acciones preventivas y correctivas, las primeras son las propia medidas de seguridad implementadas en el tratamiento del riesgo, que al seguir implementándolo continuamente se deberán ir ajustando, y las correctivas, las cuales deberán operarse una vez revisado el sistema y resultado una no conformidad, entendiendo esta como incumplimientos ya sea normativos, de las políticas, de las medidas de seguridad o del alcance de los objetivos de seguridad planteados en relación con la operación de los procesos internos del sujeto obligado.

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

   Las acciones preventivas deben atenderse considerando:

   i. El análisis y revisión de las amenazas y vulnerabilidades;
   ii. Determinar las fallas o incidentes que podría desencadenarse si una amenaza explota una vulnerabilidad de alguno de los activos;
   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.

b) **Acciones correctivas.** Son las acciones encaminadas a eliminar las causas de no conformidades, fallas, incumplimientos detectados o incidentes ocurridos en el SGSDP, con objeto de corregirlas, dichas acciones deben ser proporcionales a la gravedad de la falla o 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.

Para el caso de las acciones correctivas es posible que, si recién se ha implementado el SGSDP, sean muchas las mejoras-acciones correctivas que se deben abordar, sin embargo, es fundamental priorizarlas sobre los problemas más importantes y urgentes de resolver, y posteriormente corregir aquellas no conformidades o fallas menos trascendentes, por eso es un ciclo de mejora continua, y no se debe pretender que en dos iteraciones del ciclo el sistema sea perfecto.

La implementación de las acciones preventivas o correctivas puede establecerse en un periodo inmediato a la detección y análisis del punto de mejora o bien, otras deben esperar a finalizar el ciclo o calendarizarse en función de la importancia o criticidad de la mejora, el impacto que pueda tener dentro del sistema y los recursos disponibles. Esto es así ya que, algunas medidas pueden implementarse en el momento y no afectarán ningún otro proceso interno del sujeto obligado o del propio sistema, sin embargo, habrá acciones correctivas que deben analizarse a fondo porque quizá afecten partes fundamentales del sistema, por ejemplo, cuando se deben modificar objetivos de seguridad, políticas y programas, procesos o bien, se incluyan o modifiquen indicadores.

Finalmente, es importante tener en cuenta que las acciones de mejora deben comunicarse a las partes interesadas dentro del sujeto obligado, al ser un sistema que se integra en los procesos internos de la entidad, es indispensable que la información fluya de manera adecuada a efectos de que las correcciones tengan el efecto deseado y no perjudiquen a otras partes del sistema o algún proceso.

Una vez acometidas las acciones de mejora, se debe continuar con el ciclo.

4. SÍNTESIS DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

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 su relación con la seguridad de los datos personales y con la gestión del riesgo.

2.1 Definiciones
Definición de términos utilizados o referenciados en la guía.
2.2 Conceptos clave para comprender un sistema de gestión

¿Qué es un sistema de gestión?
¿Qué es la gestión del riesgo?
Relación entre sistema de gestión y gestión del riesgo
Estándares internacionales sobre sistemas de gestión y metodologías de gestión del riesgo

2.3 Introducción al SGSDP

Definición de objetivos y descripción de las fases que componen el ciclo de implementación de un SGSDP.

3. Implementación del SGSDP conforme al ciclo PHVA o ciclo Deming

Esquema por fases y pasos.

Fase 1. Planear el SGSDP

Paso 1. Establecer el alcance y los objetivos de acuerdo con el contexto del sujeto obligado y los criterios básicos para identificar el riesgo. Conocer el contexto de la organización para establecer el alcance del sistema de gestión y los objetivos de seguridad, asimismo en esta fase se establecen los criterios de nivel de riesgo aceptable, y de identificación del riesgo.

Paso 2. Política de Gestión y Tratamiento de Datos Personales. El compromiso formal documentado donde el responsable del tratamiento establece lo que puede realizarse, lo que no, las obligaciones y sanciones en caso de incumplimiento respecto al tratamiento de datos personales en el sujeto obligado.

Paso 3. Funciones y Obligaciones de quienes traten Datos Personales. Asignación de responsabilidades, roles y privilegios, así como la cadena de rendición de cuentas para la implementación del SGSDP.

Paso 4. Inventario de Tratamientos de Datos Personales. Identificación de los tipos de datos y su flujo, así como los sistemas y activos que los soportan.

Paso 5. Gestión del riesgo.

5.1. Valoración del riesgo

- **Identificar Activos**
- **Identificar Amenazas**
- **Identificar Vulnerabilidades**
- **Identificar Escenarios de Vulneración**
- **Análisis de riesgos**
- **Evaluación de riesgos**

5.2. Tratamiento del riesgo

- **Opciones del tratamiento: mitigar o reducir, retener, evitar, compartir y aceptar.**
- **Análisis de brecha**
- **Plan de trabajo**

Fase 2. Implementar y Operar el SGSDP
Comprender los procesos transversales al ciclo: brindar recursos, control operacional/información documentada, y sensibilización y capacitación.

Paso 6. Implementación de las Medidas de Seguridad (plan de trabajo). Operar las medidas de seguridad y trabajar en mejorar su madurez.

Fase 3. Monitorear y Revisar el SGSDP
Monitorear y revisar implicará actividades programadas como las iteraciones a la gestión del riesgo o las auditorías, pero también la revisión cuando se presenten vulneraciones de seguridad.

Paso 7. Revisión de factores del riesgo. Se deben realizar iteraciones de la gestión del riesgo.

Paso 8. Evaluación de la eficacia de las medidas de seguridad. Evaluar la eficacia de las medidas a través de métricas e indicadores con relación al cumplimiento de los objetivos de seguridad.

Paso 9. Auditorías. Se deben realizar auditorías internas y/o externas para evaluar la operación del sistema y detectar áreas de mejora para efectos de la mejora continua.

Paso 10. Revisión por el Comité de Transparencia y Directivos. Se deben establecer reuniones periódicas donde se evalúe la efectividad del sistema de gestión y se revise el progreso de las acciones requeridas para mejorarlo.

Fase 4. Mejorar el SGSP

Paso 11. Mejora Continua. De la operación del sistema y su monitoreo y revisión se desprenderán acciones preventivas y correctivas que se deben implementar para mejorar el sistema.

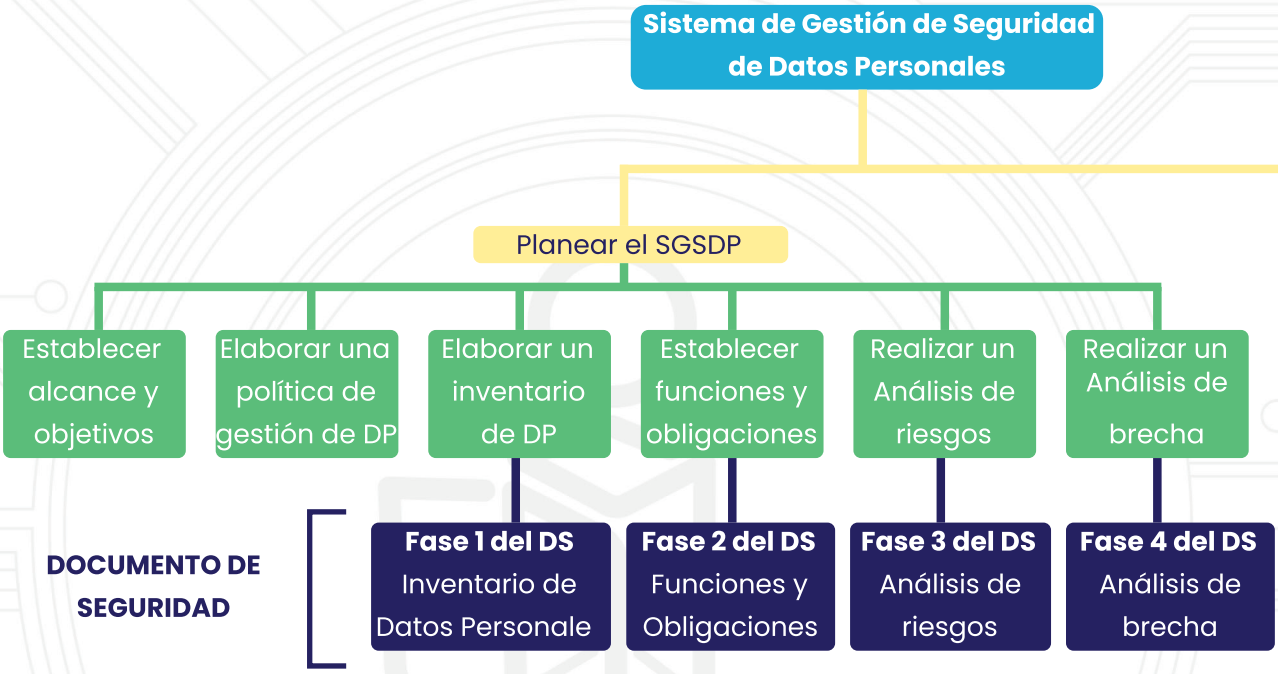
5. EL DOCUMENTO DE SEGURIDAD Y SU RELACIÓN CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

De acuerdo con la Ley General, todas las medidas de seguridad adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, deben documentarse en el Documento de Seguridad, él cual es un instrumento que describe y da cuenta de manera general sobre dichas medidas de seguridad (técnicas, físicas y administrativas)[64].

Artículo 35 de la Ley General:
"De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:
I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
II. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación."

La integración del Documento de Seguridad es recomendable se lleve a cabo una vez se ha implementado el SGSDP, en tanto que será la documentación propiamente dicha de ciertos puntos clave del sistema de gestión. Sin embargo, es posible realizar el Documento de Seguridad previo a la implementación del sistema de gestión. De hecho, en la fase de planeación del SGSDP se pueden identificar varios contenidos del documento de seguridad, a excepción de las actividades "Elaboración de una política de gestión de datos personales y "Establecimiento del alcance y objetivos.

64 Véase la Guía de apoyo para la elaboración del Documento de Seguridad. Disponible en https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf


Sistema de Gestión de Seguridad de Datos Personales
Planear el SGSDP
Establecer alcance y objetivos
Elaborar una política de gestión de DP
Elaborar un inventario de DP
Establecer funciones y obligaciones
Realizar un Análisis de riesgos
Realizar un Análisis de brecha
DOCUMENTO DE SEGURIDAD
Fase 1 del DS Inventario de Datos Personale
Fase 2 del DS Funciones y Obligaciones
Fase 3 del DS Análisis de riesgos
Fase 4 del DS Análisis de brecha

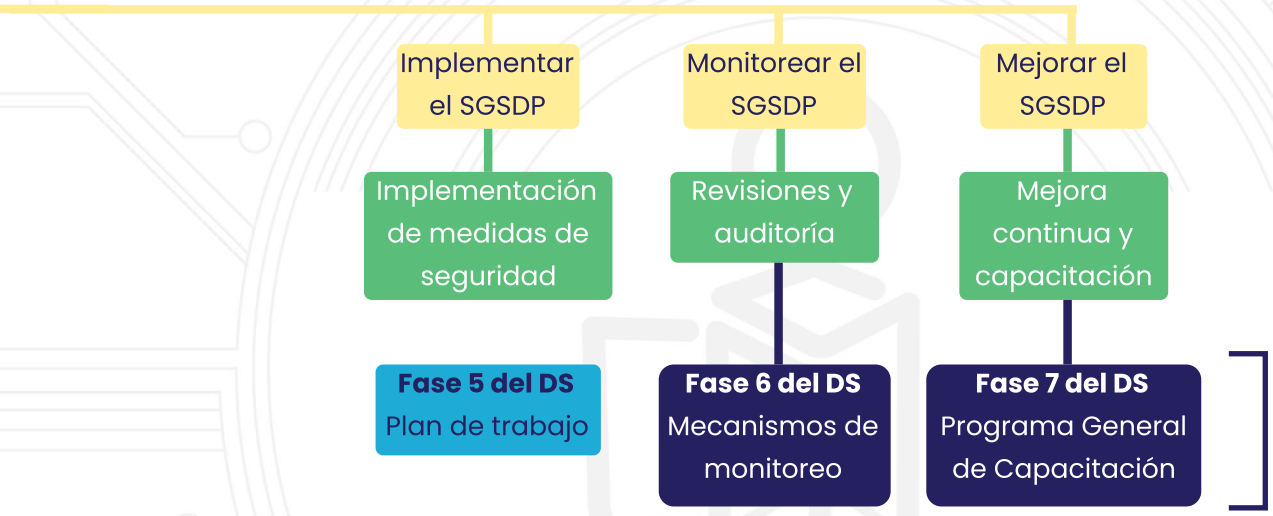


Figura 12. Esquema comparativo entre Sistema de Gestión de Seguridad de Datos Personales y Documento de Seguridad
Autoría propia

INAI México

inai.org.mx 800 835 43 24

Avenida Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Código Postal 04530, Ciudad de México.