GUÍA DE APOYO

para la elaboración del

DOCUMENTO DE SEGURIDAD

GUÍA DE APOYO
PARA LA ELABORACIÓN
DEL DOCUMENTO DE SEGURIDAD

DICIEMBRE DE 2022

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

DIRECTORIO

Secretaría de Protección de Datos Personales
Dirección General de Prevención y Autorregulación
Dirección de Seguridad de Datos Personales del Sector Público

Instituto Nacional de Transparencia,
Acceso a la Información y Protección de Datos Personales
Avenida Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Código Postal 04530, Ciudad de México

CONTENIDO

AVISO IMPORTANTE

Este documento es una referencia esquemática que describe el marco general de medidas y acciones que pueden considerarse para facilitar el cumplimiento de las obligaciones que establece la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*[1] (en adelante *Ley General*) y *los Lineamientos Generales de Protección de Datos Personales para el Sector Público*[2] (en adelante *Lineamientos Generales*) respecto a la elaboración del *Documento de seguridad*.

Las recomendaciones y sugerencias que aquí se muestran no son vinculantes para los sujetos obligados. Esta guía constituye una de las herramientas de facilitación y orientación que elabora la Dirección General de Prevención y Autorregulación de la Secretaría de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI), para apoyar a los sujetos obligados en el cumplimiento de sus obligaciones en materia de protección de datos personales.

Al ser una guía orientadora, su función principal es servir de ejemplo. Por ello resulta indispensable que, para la integración y elaboración del *Documento de seguridad*, los sujetos obligados realicen las actualizaciones, adaptaciones y precisiones necesarias según las características propias de los tratamientos de datos personales que se identifiquen en su institución.

La implementación del *Documento de seguridad* requiere de acciones generales, además de las específicas que tendrá que realizar cada unidad administrativa coordinada por el área que se designe y con el apoyo de la Unidad de Transparencia como principal asesor en materia de protección de datos personales[3]. Esto para documentar las actividades que lleven a cumplir con sus obligaciones en materia de protección de datos personales, que en el caso específico del *Documento de seguridad* se refiere a:

- Elaboración del inventario de tratamientos, que permitirá tener un diagnóstico y mapeo de los tratamientos que realiza la organización y que es necesario para cumplir con el resto de las obligaciones;
- Funciones y obligaciones de las personas que tratan datos personales;
- Elaboración del análisis de riesgo y el análisis de brecha;
- Elaboración de un plan de trabajo;

[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.

[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.

[3] Artículo 85, fracción VII. *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.

- Integración de mecanismos de monitoreo y revisión de las medidas de monitoreo y revisión;
- Elaboración o actualización del programa de capacitación para los servidores públicos en materia de protección de datos personales.

PRESENTACIÓN

La *Ley General* establece que cada responsable deberá elaborar un *Documento de seguridad*. Al tiempo lo define como un instrumento que describe y da cuenta, de modo general, sobre las medidas de seguridad, técnicas, físicas y administrativas que adopte para garantizar confidencialidad, integridad y disponibilidad de los datos personales que posee.

En ese orden, de conformidad con el artículo 35 de la *Ley General*, dicho documento debe contener al menos el inventario de datos personales y de los sistemas de tratamiento, funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación.

Por su parte, en el Capítulo Segundo de los *Lineamientos Generales* se describen los elementos mínimos a contemplar en cada uno de los contenidos del *Documento de seguridad*.

De acuerdo con los elementos señalados por el marco normativo en la materia para identificar una serie de acciones encaminadas para la integración del *Documento de seguridad*, aquí se describe su contenido a partir de los mínimos establecidos.

En ese orden, y para facilitar la integración de su *Documento de seguridad*, los títulos de análisis de riesgo y análisis de brecha se desarrollaron con el apoyo del estudio e interpretación de normas y estándares internacionales orientados a la gestión de riesgos y a la gestión de la seguridad de la información. Asimismo, otros retoman el contenido de diversos documentos publicados por el INAI, como: el *Documento Orientador para la Elaboración de Programa de Protección de Datos Personales*, la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015*, las *Recomendaciones para el manejo de incidentes de seguridad de datos personales*, y las *Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración del riesgo*. Por ello, si requiere abundar sobre algún tema específico, puede consultar los documentos señalados en el repositorio de publicaciones de protección de datos personales en la página web del INAI.

Esta guía representa un ejercicio de concreción, síntesis y armonización de las referencias señaladas.

DEFINICIONES

Las siguientes definiciones se retoman de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, *el Diccionario de Protección de Datos Personales*[4], y la *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015*[5].

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

Activo: En términos generales, un activo es cualquier elemento que representa un valor para la organización. Según la Real Academia Española, «valor» se define como: a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite, y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.

Análisis de riesgos: Permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales.

Las metodologías de análisis de riesgo establecen un proceso sistemático que consiste en crear escenarios de riesgo, identificando y correlacionando todos los elementos que intervienen en él: activo (que en el presente contexto consiste en los datos personales), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia y el nivel de impacto o de beneficio para el atacante.

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

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables y encargadas de los datos personales.

Bases de datos: 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.

[4] INAI, Davara Fernández de Marcos, Coord. (2019, noviembre), *Diccionario Protección de Datos Personales*, Conceptos fundamentales. Consultada realizada el 25/04/2022. Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

[5] INAI (2015, junio), *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, Consulta realizada el 25/04/2022. Disponible en https: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Bloqueo: Identificación y conservación 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 éstas. Durante dicho período, los datos personales no podrán ser objeto de tratamiento. Transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

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

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la *Ley General de Transparencia y Acceso a la Información Pública*.

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.

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

Custodios: Aquellas personas servidoras públicas con responsabilidad funcional sobre los activos: responsables del departamento de datos, administradores de sistemas o responsables de un proceso o proyecto 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.

Datos personales sensibles: Los que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De modo enunciativo mas no limitativo, 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.

Documento de seguridad: Instrumento que describe y da cuenta de modo general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

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

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales en nombre y por cuenta del responsable.

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

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

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.

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

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

Responsable: Los sujetos obligados (a los que se refiere el artículo 1º de la *Ley General*) que deciden sobre el tratamiento de datos personales.

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

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

Riesgo de seguridad: Combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

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.

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: Son sujetos obligados por la *Ley General*. En el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Titular: 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, responsable o encargado.

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

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

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

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

INTRODUCCIÓN

La presente Guía orienta en la elaboración del *Documento de seguridad* previsto en el artículo 35 de la *Ley General*, que establece una de las obligaciones de los responsables del sector público en el tratamiento de datos personales para cumplir con el deber de seguridad y que debe estar registrada en un *Documento de seguridad*.

La Guía está construida para servir de apoyo en las acciones a realizar con el fin de integrar un *Documento de seguridad*, considerando elementos de un sistema de gestión que permita proveer los elementos y actividades de dirección, operación y control de los procesos de la organización para proteger de modo sistemático y continuo los datos personales que estén en su posesión.

Para su elaboración, se identificaron las obligaciones que establece la *Ley General* y los *Lineamientos Generales* para todo sujeto obligado. Así, se delimitaron las acciones a seguir.

El Documento de seguridad y el sistema de gestión

El *Documento de seguridad* se define como el instrumento que describe y da cuenta de modo general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El sistema de gestión se identifica como el 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 *Ley General* y las demás disposiciones que le resulten aplicables en la materia.

De este modo, puede apreciarse una clara relación entre la implementación de un sistema de gestión y la elaboración del *Documento de seguridad*, evidenciando que es necesario empatar los contenidos que se generan al llevar a la práctica un sistema de gestión y redactando el *Documento de seguridad*, pues son actividades que pueden ir de la mano, o bien elaborarse de modo independiente, buscando que exista una concordancia de contenidos que respalden las actividades que se realizan y documentan. Por ello, puede verse al *Documento de seguridad* y al sistema de gestión de dos maneras:

- La primera: El *Documento de seguridad* surge como consecuencia de la documentación de algunos pasos de la implementación del sistema de gestión.
- La segunda: El *Documento de seguridad* es un preludio a la implementación del sistema.

Es decir, se realizó la documentación respecto a elementos de seguridad que pueden ser la base de la ejecución de los pasos necesarios para la implementación del sistema de gestión.

Considerando la precisión realizada y partiendo de la premisa de que hay contenidos que

pueden ser considerados como parte de la implementación de un **Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar)**, se identifican diversas actividades que son coincidentes para la elaboración del *Documento de seguridad* y la implementación del sistema de gestión, identificadas en el artículo 34 de la *Ley General* y el artículo 65 de los *Lineamientos Generales*, que consignan:

Artículo 34 de la *Ley General*:

«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.»

Artículo 65 de los *Lineamientos Generales*:

«Sistema de Gestión

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.»

En ese sentido, los responsables y encargados, así como todo interesado, encontrarán en esta guía los pasos claves para elaborar un *Documento de seguridad*, incorporando elementos que forman parte de un SGSDP basado en el ciclo PHVA.

Importante

El objetivo general de este documento es orientar a los responsables y encargados en la elaboración de un *Documento de seguridad* con los elementos mínimos establecidos en la normativa aplicable. Es importante asentar que la aceptación, integración y elaboración de contenidos serán determinados a partir de la definición del alcance y objetivos de cada sujeto obligado.

Esta guía retoma elementos de seguridad a través de la gestión del riesgo de los datos personales, entendiéndose de modo 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, pueda evaluarse el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal que trate.

Deberá considerarse que cada elemento del *Documento de seguridad* estará sujeto a los alcances definidos para la protección de los datos personales y su tratamiento legítimo, controlado e informado, buscando en todo momento garantizar la privacidad y el derecho a la autodeterminación informativa de las personas titulares de los datos personales. Por lo cual, la elaboración de inventarios de datos personales y sistemas de tratamiento, el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de la presente guía deberán enfocarse 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 *Ley General*.

Finalmente se aclara que lo establecido en la presente guía es de carácter orientador, por lo que los responsables y encargados podrán decidir libremente qué metodología es conveniente aplicar al interior del sujeto obligado para garantizar la seguridad de los datos personales. Asimismo, el seguimiento de la presente guía no exime a los responsables y encargados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos, ya que la seguridad de dichas bases depende de una correcta implementación de las medidas o controles de seguridad.

A partir de la siguiente sección se desarrollan los pasos para la elaboración del *Documento de seguridad* y se proporcionan los elementos básicos para ello. De este modo, los sujetos obligados deberán considerar sus características específicas y valorar la adaptación de las medidas descritas en esta Guía a sus necesidades.

ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

Debemos partir de la definición de *Documento de seguridad*, se trata de aquel documento elaborado por el sujeto obligado que contiene las medidas de seguridad administrativas, físicas y técnicas aplicables a sus sistemas de datos personales, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

A la hora de registrar cada uno de los contenidos del *Documento de seguridad*, es indispensable que esto se realice con toda honestidad y lo más apegado a la realidad posible, pues en él debe plasmarse la realidad sobre el tratamiento de los datos personales en la entidad, a fin de que su contenido sea utilizado para una mejor toma de decisiones respecto a las acciones a implementar de modo específico para mejorar dicha seguridad. No tiene caso elaborar acciones impecables o de imposible cumplimiento.

Este documento tiene como propósito identificar el universo de sistemas de tratamiento de activos de información, que en este caso son los datos personales que posee cada dependencia o entidad, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y los activos de apoyo, que son los soportes físicos y/o electrónicos en los que reside la información tratada por cada sistema de tratamiento declarado; además de identificar todas las medidas de seguridad concretas implementadas para el resguardo de los datos que se tratan.

El **Documento de seguridad deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos** de las dependencias y entidades, **así como para las personas externas que, debido a la prestación de un servicio, tengan acceso a tales sistemas de tratamiento** o al sitio donde se ubican los mismos.

Para lograr la elaboración del *Documento de seguridad* y en su caso, la implementación de un Sistema de Gestión de Seguridad de Datos Personales, es imprescindible la cooperación de todas las Unidades Administrativas del sujeto obligado y de las personas propietarias y custodios de los datos personales, o bien, que velen por la seguridad de la información que contiene dichos datos.

A continuación se exponen las actividades a realizar para documentar las secciones que integran un *Documento de seguridad*, según el artículo 35 de la LGPDPPSO. No obstante, es importante señalar que dicho artículo no cuenta con desarrollo en los *Lineamientos Generales*, aunque sí se desarrollan sus contenidos a partir del artículo 57 de dicho cuerpo normativo, en relación con el artículo 33 relativo a las acciones que deben realizar los responsables a efectos de imponer las medidas de seguridad para la protección de datos personales, y que es en esencia lo que se busca con el *Documento de seguridad* y con el SGSDP.

ETAPA 1

EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

En esta etapa se busca documentar un listado de todos los sistemas de tratamiento físicos y electrónicos donde se efectúe tratamiento de datos y se realice una clasificación de todos los datos personales.

Los sujetos obligados deberán elaborar un inventario de datos personales y de los sistemas de tratamiento, conforme a lo dispuesto en la *Ley General* y los *Lineamientos Generales*. Por ello se recomienda atender 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.»

Importante

Es obligación de los sujetos obligados mantener actualizado un inventario de los sistemas de tratamiento de datos personales que utiliza su organización. Por ello es necesario involucrar a cada área que realiza el tratamiento, pues ellas son las 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 modo directo 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 1. Ciclo de vida de los datos personales.

El inventario de datos es parte de las acciones encaminadas a garantizar la seguridad de los datos personales, por lo que puede entenderse como el control documentado que se llevará de los tratamientos que realizan las áreas de la organización, 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.

Además de las facultades legales, se debe identificar el fundamento jurídico 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 diversos 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 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?

Diversas personas pueden tener acceso a los sitios donde se almacenan los datos personales. Éstas 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 deberá identificarse 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.

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

Para identificar los tipos de datos personales que se tratan y los formatos en los que se encuentran, es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo. Éste se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realiza en su institución.

Por «inventario de tratamientos de datos personales» se entenderá el control documentado que cada unidad administrativa llevará de los tratamientos que realiza al interior de la institución. Este catálogo deberá ser elaborado con orden y precisión. El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los *Lineamientos Generales* identificará los siguientes elementos relevantes:

¿Qué tratamientos de datos personales realiza la unidad administrativa?

Debe identificarse 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?

Es importante identificar o definir si la unidad administrativa está a cargo del proceso donde se tratan los datos personales, según las atribuciones o facultades normativas.

Por ejemplo, un sujeto obligado cuenta con una Dirección de reclutamiento y otra de Administración de Personal. La primera puede conocer los documentos como *currículum vitae*, exámenes de control de confianza, referencias laborales, nombres de patrones previos, pero no conocerá el 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 corresponde por facultades a la Dirección de Administración de personal. No obstante, esta segunda Dirección sí conoce 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 modo conjunto.

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.

Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

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

En este paso deben identificarse los medios de obtención de los datos personales, pues existen diversas maneras por las cuales pueden obtenerse los datos personales:

- Directamente del titular
    - De modo 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.

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 ésta.

- 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 por o tenga una procedencia ilícita, según 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 ello, puede contestar estas 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 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 modo enunciativo mas no limitativo, se refieren a aquéllos 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 almacena y realiza el tratamiento de los datos personales?

Se elaborará un catálogo de los tipos de datos personales que se tratan. Se identificará el tipo de dato personal que almacena. Se consignan al menos los siguientes elementos:

- **Formato en que se encuentra la base de datos: Primero debe considerar 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. Esto es, asentar si la base de almacenamiento de datos se encuentra en formato físico y/o electrónico.

- **Ubicación de la base de datos:** Consignar 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

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser «contratación de personal»; y las finalidades, «evaluación de currículum para la selección de personal».

Así, es necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito). En caso de que no se requiera, debe definirse 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, detallando 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;
- Los privilegios que tiene cada usuario sobre 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 tienen encargados fuera del sujeto obligado para el tratamiento de datos personales. De ser así, debe integrarse el nombre del encargado y el nombre o número de contrato, pedido o convenio correspondiente. Estos datos pueden encontrarse en el instrumento jurídico que formaliza la prestación de servicios.

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, responsable o encargado. Por ello, debe 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, es necesario precisar los siguientes elementos:

- Identificar 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 tal caso, debe indicarse 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 ello 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 modo 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 éstos

El bloqueo se refiere a la identificación y conservación 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 éstas. Durante dicho período, los datos personales no podrán ser objeto de tratamiento. Transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Para conocer el formato propuesto por el INAI que incluye los elementos enlistados y poder consultarlo y llenarlo con mayor detalle, revise el *ANEXO A. Formato de Inventario de datos personales y sistemas de tratamiento* de este documento.

ETAPA 2

LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Una vez que se tiene desarrollado el inventario de datos personales y sistemas de tratamiento, se tendrá oportunidad de identificar a los servidores públicos que intervienen durante el procesamiento y aprovechamiento de los datos personales. Entonces se tiene conocimiento pleno de quiénes tratan datos personales, y las actividades que realizan durante el tratamiento declarado.

La identificación de todas las personas que intervienen en el tratamiento de datos personales a lo largo de su ciclo de vida debe ser congruente con sus roles y responsabilidades. De acuerdo con el caso deben otorgarse los privilegios de tratamiento; de lo contrario, una asignación no adecuada puede producir voluntaria o involuntariamente la afectación a la confidencialidad, integridad o disponibilidad de los datos personales.

Es muy importante que las obligaciones y responsabilidades que tiene cada puesto en el tratamiento de datos personales queden claramente definidas, además de considerarse en las políticas de seguridad de la información acuerdos de confidencialidad, o bien en los términos y condiciones de la relación laboral, según sea el caso. A partir de lo anterior, es necesario que se establezcan mecanismos para dar a conocer a todos los servidores públicos que intervienen en el tratamiento de datos personales cuáles son las funciones, obligaciones y posibles sanciones de quienes incurran en una conducta que derive en una potencial vulneración a los datos personales del sistema asignado.

Es así como, de acuerdo con la *Ley General* y a los *Lineamientos Generales*, los sujetos obligados deberán observar 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. 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 otras palabras, para atender este rubro, el sujeto obligado deberá definir y dar a conocer a su personal una serie de documentos o mecanismos que permitan identificar de modo claro y preciso los siguientes elementos:

- Funciones del personal involucrado en el tratamiento de datos personales en cualquier fase del tratamiento;
- Obligaciones del personal que trate datos personales en cualquier fase del tratamiento;
- Posibles sanciones por el incumplimiento de las funciones y obligaciones establecidas.

ETAPA 3

EL ANÁLISIS DE RIESGOS

Debe contarse con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades para los datos personales y los recursos involucrados en su tratamiento. Pueden ser, de modo enunciativo mas no limitativo: *hardware*, *software*, personal del responsable, entre otros.

El responsable de esta actividad deberá 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.

Los beneficios de contar con un análisis de riesgos son grandes y algunos de ellos son: soporte a decisiones estratégicas, apoyo en la definición y asignación efectiva de recursos, justificación de esfuerzos en tiempo, recursos humano y financieros, promoción de la mejora continua, transmisión de confianza y servicio como uno de los pilares de los Sistemas de Gestión de Seguridad de la Información.

¿Qué es un riesgo?

De acuerdo con la *Guía para implementar un SGSDP Junio 2015*[6], 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[7].

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 ello, cuando un riesgo se materializa ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

[6] INAI, (2015, junio), *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, Consulta realizada el 25/04/2022. Disponible en https: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

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

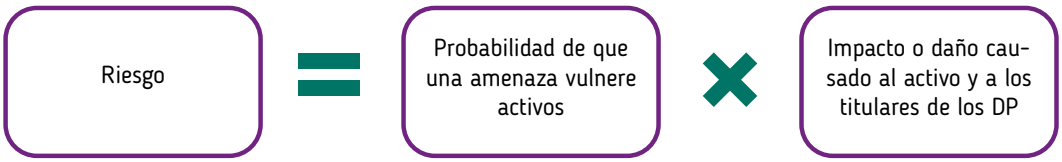


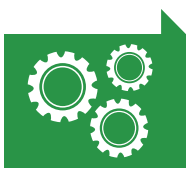
Figura 2. Elaboración propia.

¿Qué es un riesgo inherente?

Según la definición técnica, el riesgo inherente es la valoración del grado de exposición de un activo a una amenaza que pueda explotar su vulnerabilidad, sin considerar 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, causando un mayor impacto en los titulares y/o en sus derechos y libertades.

El riesgo inherente en los sistemas de tratamiento de datos personales puede incrementar 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.



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

Disociación: Se aíslan los datos de modo que por sí no aporten información valiosa de un titular o éste no pueda ser identificable. Así, el valor de la base de datos para una persona no autorizada se ve disminuido.

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

Es importante identificar este tipo de riesgo para ayudar a cuantificar el riesgo a partir del nivel de interés que puede generar en un atacante.

La gestión de los riesgos

Una vez que se sabe que es un riesgo, hay que ponerlo en contexto con la protección de datos personales, donde nos referimos a la posible vulneración de datos y a la intimidad de las personas, traduciéndose como una consecuencia no deseada sobre los interesados, capaz de generar daños o perjuicios a las personas titulares.

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales. No obstante, el riesgo no puede erradicarse completamente, pero sí minimizarse a través de la mejora continua. El análisis de riesgos no debe entenderse como un documento, sino como un proceso que se ejecuta a través de hechos y se acredita documentalmente.

En este punto, es importante identificar al análisis de riesgos como una actividad que forma parte de un proceso más grande conocido como gestión de riesgos, donde se establece una serie de actividades a realizar, divididas en etapas, buscando siempre minimizar los riesgos a los que se enfrentan los sistemas en que se resguardan los datos personales. Por ello, este documento parte de la estructura identificada en la gestión de riesgos.

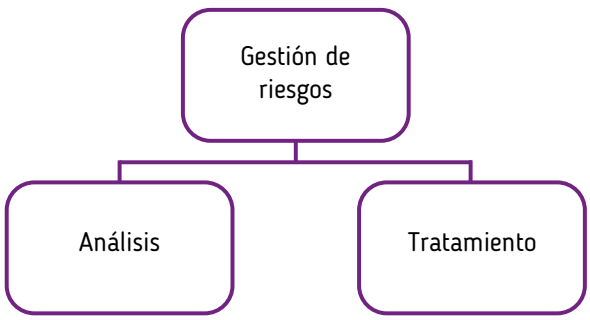


Figura 3. Elaboración propia.

La combinación del análisis y el tratamiento de riesgos da como resultado un proceso llamado **Gestión de riesgos**, donde se busca:

1. Determinar qué activos tiene la organización y estimar lo que podría pasar;
2. Organizar de modo informado una serie de actividades preventivas, evitando que ocurra un incidente con miras a que, al mismo tiempo, se esté preparado para una emergencia.

A continuación, se presenta un diagrama[8] del proceso de gestión de riesgos más exhaustivo, en materia de seguridad de la información.

[8] Ministerio de Hacienda y Administraciones Públicas (2012, octubre). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. MAGERIT-versión 3.0, Libro I, Glosario. P. 20. Fecha de consulta: 28/04/2022. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

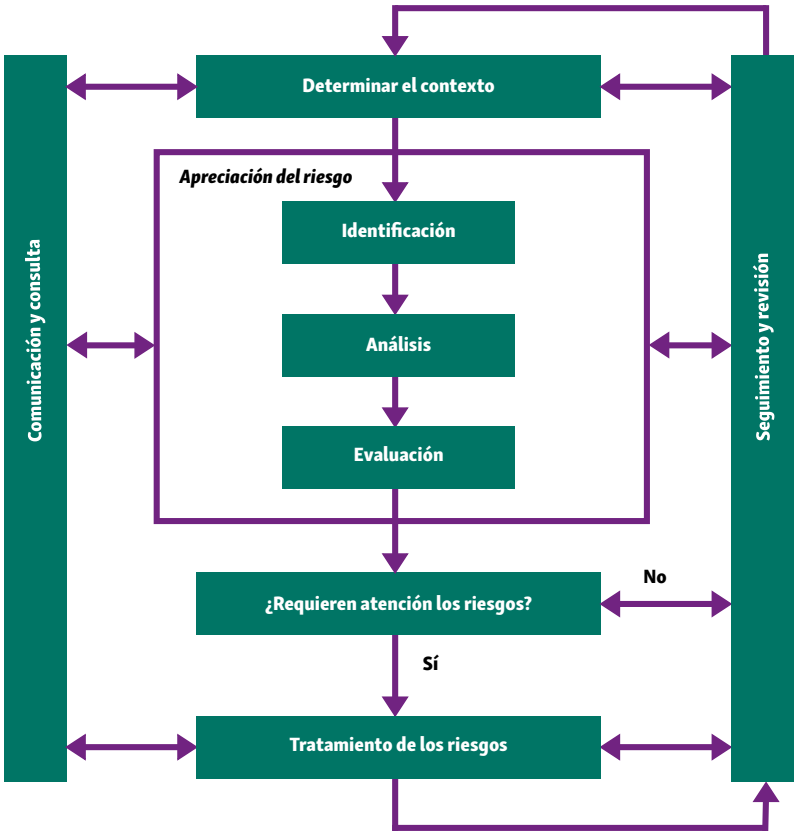


Figura 4. Diagrama MAGERIT.

¿Cómo realizar el análisis de riesgos?

El análisis de riesgos es un proceso sistemático para conocer y determinar la magnitud de los riesgos a los que se encuentran expuestos los activos de responsable. El análisis de riesgos permite determinar cómo es, cuánto vale y cómo está protegido cada activo (identificando posibles problemas), y anticiparse a las futuras dificultades, lo que nos permitirá tomar mejores decisiones y actuar con oportunidad.

En el análisis de riesgos deben considerarse los siguientes elementos:

- **Activos**, que se dividen en dos tipos:
  - Activos de información: Datos personales;
  - Activos de apoyo: Elementos físicos e infraestructura que soportan los activos de información;
- **Amenazas**: Eventos con la capacidad de causar daño a una organización;
- **Vulnerabilidades**: Debilidades de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Con los elementos enlistados pueden estimarse el impacto (lo que puede pasar) y el riesgo (la probabilidad de que la amenaza vulnere el activo). Es decir, en el análisis de riesgos se deben mapear escenarios donde se visualice cómo las amenazas aprovechan una o diversas vulnerabilidades de los activos, estimando qué tanto puede impactar de modo negativo en los activos. Así se estiman los riesgos; en este caso, los activos serán los datos personales y los sistemas y recursos que los soportan, como pueden ser, de modo enunciativo mas no limitativo: *hardware*, *software*, personal del responsable, entre otros.

El resultado del análisis de riesgos permite tener elementos con fundamento para proceder al tratamiento de los riesgos.

El responsable de realizar el análisis de riesgos debe considerar los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico, el valor de los datos personales según 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 la ocurrencia de una vulneración de seguridad.

Para llegar a esta actividad es muy importante que se tenga bien definido el inventario de datos personales o sistemas de tratamiento. Esto porque a partir de la descripción de este inventario se podrán identificar elementos necesarios como el formato en que se encuentra la base de datos generada en la descripción de los sistemas de tratamientos para realizar sus análisis de riesgos.

Importante

Todos los ejemplos cuantitativos y cualitativos se basan en las Metodologías ISO IEC/27005 y MAGERIT-versión 3.0, donde se advierte también que son escalas sugeridas. Las metodologías mencionadas proporcionan pautas para la gestión de riesgos de seguridad de la información, que a su vez son compatibles con el sistema de gestión de seguridad de la información descrito en la ISO IEC/27001.

En esta sección, los responsables podrán determinar las características del riesgo que mayor impacto puede tener sobre los datos personales que tratan, y por lo tanto que puedan tener sobre las personas titulares de éstos, con el fin de que prioricen y tomen la mejor decisión respecto a los controles o medidas de seguridad más relevantes e inmediatas a implementar.

Conforme a la *Ley General y los Lineamientos Generales*, para el tema de análisis de riesgos, los sujetos obligados deberán atender 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. [...]

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 modo enunciativo mas no limitativo, *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 con 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*.»

Metodologías para el análisis de riesgos

Una vez comprendido lo que es un riesgo y los elementos que interactúan en la elaboración del análisis de riesgos, se debe fijar una metodología, por lo que es importante definir lo que se entiende como metodología.

Una metodología de análisis de riesgos se entiende como un conjunto de técnicas empleadas para evaluar los riesgos. Es decir, acciones que permiten cuantificar la magnitud de los diversos riesgos a los que puede enfrentarse un sistema de tratamiento, a partir de la evaluación de los riesgos.

Cuando hablamos de las metodologías para realizar el análisis e incluso la gestión de riesgos, podemos identificar una gran variedad de éstas. Cada responsable puede utilizar la metodología que considere más conveniente, a partir del conocimiento de los activos que va a analizar. De este modo, deberá considerar que es posible adoptar una metodología en concreto, o bien seleccionar 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 considerar que algunas de estas metodologías son más idóneas para las condiciones del análisis. Además, se debe contar con bibliografía especializada y personal capacitado en la gestión de riesgos para la interpretación y aplicación de los contenidos, lo cual pudiera representar un gasto para el s1ujeto obligado.

En ese sentido, y con el objetivo de brindar a los sujetos obligados un documento básico que oriente sobre los elementos y contenidos de modo general de las metodologías de análisis de riesgos para la realización de éstos, se llevó a cabo una revisión genérica de los puntos clave de algunas metodologías orientadas al análisis de riesgos, a fin de identificar las características de cada una. Se tuvo como resultado lo siguiente:

MAGERIT V3[9]
El análisis 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 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.

[9] Ministerio de Hacienda y Administraciones Públicas (2012, octubre). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. MAGERIT-versión 3.0, Libro I. Flecha de consulta: 28/04/2022 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

METODOLOGÍA BAA[10]

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 atacante.

A partir de lo anterior, se ha dado el nombre «BAA» a esta metodología de análisis de riesgos. Los pasos 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 medidas 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.

[10] INAI (2015, junio). *Metodología de Análisis de Riesgo BAA*. Fecha de consulta: 28/04/2022. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_Análisis_de_Riesgo_BAA(Junio2015).pdf

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS SEGÚN ISO 31000:2018[11]

El proceso propuesto por la ISO 31000:

Comunicación y consulta

Esta fase es importante dado que en ella dan sus opiniones acerca del riesgo con base en la percepción de cada una de las partes involucradas. La comunicación y la consulta deben 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 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, cuáles 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 éstos, cuyos resultados quedan registrados en informes.

Registro

Los registros brindan la base para la mejora de los métodos y las herramientas, así como del proceso global.

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

[11] Consulta realizada el 28/04/2022. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Dicho lo anterior, es fundamental que considere que cualquiera de las metodologías mencionadas para el análisis de riesgos requiere que el responsable destine recursos materiales, financieros y humanos orientados a la especialización en la gestión de riesgos de aquéllos que realicen esta actividad. Esto para llevar a cabo una correcta implementación del análisis de riesgos.

Por lo expuesto, este documento no puede determinar qué metodología es mejor, ya que se debe partir de que todas tienen el mismo objetivo. A partir de la comparación, pueden identificarse puntos en común o pasos a seguir, los cuales conformarían una base mínima para un análisis de riesgos no especializado.

Debido a que este documento parte de la idea de que los elementos del *Documento de seguridad* son compatibles con los resultados de los pasos realizados durante la aplicación de un sistema de gestión de seguridad de la información orientado a datos personales, se sintetiza, conjunta y toma como base elementos coincidentes de varias metodologías de análisis de riesgos. La primera es la *Guía de Gestión de riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia*[12], que a su vez se basa en los estándares internacionales ISO/IEC 27001 e ISO/IEC 27005; la segunda, Risk Management of Information Security, (en español, Gestión de Riesgos de la Seguridad la Información), MAGERIT versión 3.0[13]. Para la elaboración de su análisis de riesgos, debe contemplar las siguientes acciones:

1. **La determinación del contexto:** Es decir, tomar una decisión de los parámetros y condicionantes externos e internos que permitan encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, que sean para intercambio de información y servicios o proveedoras de servicios subcontratados.

2. **La identificación de riesgos:** Buscar los puntos de peligro. Lo que identifique pasa a la etapa de análisis de riesgos; lo que no, puede ser calificado como riesgo oculto o ignorado.

- En esta fase deben identificarse y valorarse los activos, a efecto de visualizar cuáles son los de mayor criticidad para la operación del sujeto obligado. Posteriormente se analizarán las amenazas a las que están expuestos así como sus vulnerabilidades,

[12] Ministerio de Tecnologías de la Información de Colombia (2016, abril). *Guía de Gestión de Riesgos, Seguridad y Privacidad de la Información*. Fecha de consulta: 03/05/2022. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

[13] Ministerio de Hacienda y Administraciones Públicas (2012, octubre). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT-versión 3.0*. Fecha de consulta: 03/05/2022. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

para calcular la probabilidad de que el riesgo se materialice, y el impacto que ello causaría a los activos y por lo tanto a los titulares de los datos personales. Entra aquí la **identificación de activos** de información y de apoyo, en el caso particular, orientado a los datos personales y sistemas de tratamiento que los soportan.

- Sobre estos activos de apoyo, donde se encuentran los datos personales, se hace la **identificación de las amenazas** (circunstancia o condición externa, con la capacidad de causar daño a los activos, explotando uno o más de sus vulnerabilidades).
- Posteriormente, se hace la **identificación de las vulnerabilidades** (circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño), ya que, cuando se materializa una amenaza y hay una vulnerabilidad que pueda ser aprovechada, hay una posibilidad a que se presente algún tipo de pérdida. La presencia de vulnerabilidades no causa daño por sí misma: se requiere una amenaza que la explote. De este modo, es necesario crear un escenario de vulneración a partir de la identificación de las consecuencias de las posibles vulneraciones. Es decir, identificar el daño o impacto de que ocurra la vulneración. El impacto se determina considerando el grado de daño en los activos, y en el caso particular debe valorarse también el impacto negativo a los titulares de los datos personales.
- Posteriormente, debe calcularse la probabilidad de ocurrencia de la vulneración (el incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento).
- Finalmente, debe calcularse el riesgo intrínseco de los activos concernientes a datos personales y sistemas de tratamiento que los soportan.

3. **El tratamiento de los riesgos** recopila las actividades encaminadas a modificar la situación de riesgo en que se encuentran los activos.

El análisis de riesgo deberá arrojar como resultado un valor del riesgo para cada uno de los escenarios de vulneración analizados por cada activo de apoyo identificado.

Definición del alcance, contexto y objetivos del análisis de riesgos

Una vez definida la metodología a utilizar, y previo a la identificación de los activos, se debe definir el alcance y objetivos del análisis de riesgos como parte de la gestión de riesgos. Por ello debe realizar lo siguiente:

1. **El alcance:** Es decir, la forma en que se describen los límites del proyecto, su cobertura, sus resultados y sus entregables. Al definirlo debe ser claro en su importancia, para ser comprendido por el equipo y la dependencia o entidad. De este modo, con el alcance y los límites identificados, el equipo de análisis y la entidad serán capa-

ces de determinar los bienes, personas, procesos y las instalaciones que estarán involucrados en la actividad de análisis y evaluación del riesgo.

Un ejemplo puede ser el alcance del análisis de riesgos de los sistemas de tratamiento de la Dirección General de Administración o su equivalente de la organización, mismo que solamente involucra los sistemas físicos y digitales de tratamiento de datos personales generados a partir del ejercicio de atribuciones de dicha dirección general.

2. **El contexto:** Es esencial que la gestión de riesgos se integre con el resto de las Unidades Administrativas como con su entorno. Por ello hay que definir el marco de trabajo, teniendo en cuenta a nivel interno la cultura, los recursos económicos y humanos, así como los procesos y los objetivos sustantivos y valores de la entidad.

   En esta fase deben establecerse los criterios que se emplearán para la evaluación de los riesgos; en particular, los criterios para valorar la probabilidad y los criterios para el impacto. Asimismo tienen que establecerse y delimitarse los roles y responsabilidades. Para esto último, es posible utilizar el documento 2 que integra el Documento de seguridad «Las funciones y obligaciones de las personas que traten datos personales».

3. **Nivel de Riesgo Aceptable (NRA):** En este punto deberá fijarse el criterio sobre el NRA. Éste se refiere al nivel en una escala cuantitativa y cualitativa que será el nivel máximo de riesgo para aceptar dentro de la entidad. Esto debe fijarse a través de considerar los criterios y parámetros que exige la *Ley General*, y de modo general a los niveles de riesgo que un sujeto obligado se fije como meta respecto a sus alcances y objetivos.

   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 bajo o muy bajo (depende de la escala cuantitativa y cualitativa establecida). Sin embargo, en caso de que el sujeto obligado considerara aceptar un riesgo mayor —por cuestiones del contexto de la entidad, de los recursos humanos, administrativos y económicos—, es decir medio o alto (no se recomienda en ningún caso aceptar uno muy alto), deberá ser acordado y aceptado formalmente por el Titular de la unidad administrativa correspondiente o propietario del Tratamiento, 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.

4. **Los criterios de impacto y probabilidad:** 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) o bien que cause la pérdida o afectación de los datos personales y por lo tanto genere daños o afectaciones a las personas titulares.

Si bien debe analizarse 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 Documento de seguridad y del Sistema de Gestión de Seguridad de Datos Personales, en tanto que éste 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 ello, al valorarse el impacto a los datos personales, y por lo tanto a las personas titulares, deben considerarse, por ejemplo, sin ser éste 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.

La escala y los criterios del impacto deben quedar fijados en esta etapa. Pueden utilizarse los mencionados como ejemplo en el apartado «Valoración del riesgo». El criterio de probabilidad se refiere a la posibilidad de ocurrencia de un hecho o acontecimiento. En este caso, es la posibilidad de ocurrencia de que una amenaza aproveche la vulnerabilidad de un activo.

La probabilidad deberá valorarse en una escala temporal traducida a una cuantitativa y cualitativa, tomando como referencia la frecuencia de ocurrencia de las amenazas. Para estimar la frecuencia, podemos basarnos en datos empíricos (datos objetivos) del histórico del sujeto obligado, o en opiniones de expertos (datos subjetivos).

5. Deben establecerse **objetivos**: Es decir, establecer las metas que se quieren conseguir. Por ello deben ser específicos, medibles o evaluables, alcanzables, relevantes y deben tener un tiempo definido, lo que permitirá la evaluación de resultados y la mejora continua.

Identificar activos

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, un activo es «todo bien o re-

curso 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.»[14]

En ese sentido, los activos que tienen valor y requieren resguardarse son los datos personales, recordando que estos activos conviven con otros activos, como servicios, aplicaciones (*software*), equipos (*hardware*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

De este modo, pueden identificarse dos tipos de activos:

- Activos de información: Corresponden a la esencia de la entidad o sujeto obligado:
  - Información relativa a los datos personales;
  - Información de procesos del negocio, en los que interviene el flujo de datos personales, actividades involucradas en el tratamiento de éstos;
- Activos de apoyo, en los cuales residen los activos de información:
  - Hardware;
  - Software;
  - Redes y telecomunicaciones o personal;
  - Estructura organizacional;
  - Infraestructura adicional.

Importante

En este paso es posible utilizar el inventario de datos personales y sistemas de tratamiento. Se recomienda que, para realizar el análisis 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.

Para la identificación de activos se recomienda:

a. Detectar todos los activos de información y de apoyo del sistema de tratamiento que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales en resguardo de su institución.
Dentro de estos activos podrá incluir información documentada en papel o

[14] AEPD (2021, junio), *Gestión del riesgo y evaluación de impacto en tratamiento de datos personales*. Fecha de consulta: 28/04/2022. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

formato electrónico, aplicaciones, bases de datos, personal, *hardware*, *software*, infraestructura tecnológica, instalaciones y servicios o procesos externos.

b. Determinar el valor del activo en función de los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad[15], aplicándose una escala, por ejemplo, del 1 al 3, donde 1 es el valor más bajo y 3 el más alto. Esta valoración resulta necesaria para conocer el riesgo inherente de cada dato que conforma el sistema de tratamiento.

c. Calcular el valor del activo. Por ejemplo, sumando los valores asignados a la confidencialidad, integridad y disponibilidad, empleándose los siguientes rangos para obtener el valor (cualitativo y cuantitativo) final. En este punto deberá identificar el valor de su inventario. Considere que, si su tratamiento incluye datos sensibles, éstos deberán ser considerados con el valor más alto, debido a su naturaleza.

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

Tabla 1. Ejemplo de escalas cuantitativas y cualitativas. Elaboración propia.

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

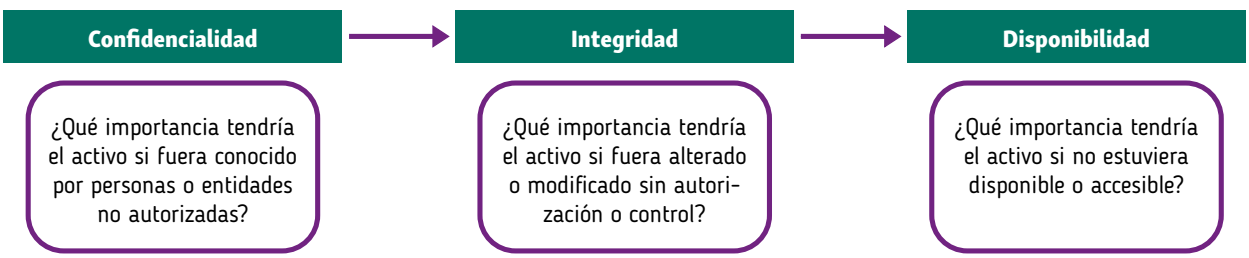


Figura 5. Elaboración propia.

[15] Metodologías como MAGERIT sugieren contemplar, además de los principios o dimensiones de confidencialidad, integridad y disponibilidad, los de autenticidad y trazabilidad. Según el Glosario de MAGERIT, se entiende la autenticidad como la propiedad o característica consistente en que una entidad es quien dice ser, o bien que garantiza la fuente de la que proceden los datos. La trazabilidad es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Sin embargo, al ser un documento guía, se establecen los mínimos requeridos.

Una vez 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:

Activo	*Valor del activo por dimensión*			*Valor total cuantitativo*	*Valor total cualitativo*
	Confidencialidad	*Integridad*	*Disponibilidad*		
Currículum Vitae en papel: contiene nombre completo, dirección particular, teléfono particular, experiencia laboral, historia académica.	3 Justificación: La divulgación o conocimiento por personas no autorizadas podrían traer consecuencias para el titular, en tanto que se podría hacer mal uso de su información personal, pudiendo incluso dañar su integridad.	2 Justificación: La alteración o modificación de los datos contenidos puede traer consecuencias legales para el titular, en tanto que podría alterarse su historia académica o experiencia laboral.	1 Justificación: No tenerlos disponibles no afecta de modo importante a la operación del sujeto obligado, salvo en ocasiones particulares.	6	Medio

Tabla 2. Valor del activo por dimensión. Elaboración propia.

Respecto al ejemplo anterior, no es necesario justificar en una tabla los valores cuantitativos. Sin embargo, sí debe estimarse con razonamientos lógicos: por ello se ha puesto la justificación del valor como ejemplo.

Por cada activo se deberá identificar un propietario. Es decir, una persona o entidad (área que trata los datos personales) con la responsabilidad y la autoridad para gestionar un activo (por ejemplo, el titular del área). El propietario del activo deberá determinar el valor de éste. En su caso, también se deberá identificar el custodio (la parte operativa). Las categorías para los sistemas de tratamiento son sólo una orientación. Es importante remarcar que ciertos datos personales que en principio no se consideran sensibles podrían llegar a serlo, dependiendo del contexto en que se trate la información.

Identificar amenazas

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

Las personas custodias de los activos y sus usuarios pueden proporcionar asesoría para identificar y estimar las amenazas relacionadas; por ejemplo, del área de recursos humanos, de los administradores de tecnologías y seguridad, profesionales en seguridad física, del departamento legal, externos como compañías de seguros, gobiernos y autoridades nacionales, entre otras fuentes informativas de investigación. Los aspectos culturales también deben ser considerados dentro de las amenazas.

Las amenazas son acciones que ocurren y pueden dañar 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 podría ocurrirle.

En este paso se recomienda realizar las siguientes actividades:

a. Identificar todas las amenazas relacionadas con cada activo. Las amenazas se identificarán utilizando los catálogos definidos para tal fin;
b. Se debe considerar que cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada con varias vulnerabilidades;
c. Se recomienda que la identificación de amenazas sea realizada por las personas propietarias de los activos, con el apoyo de las personas custodias.

Según las diversas metodologías de gestión de riesgos explicadas en este documento, las amenazas pueden dividirse en diversos grupos. Se ejemplifican tres grandes grupos con algunos ejemplos de los tipos de amenazas. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas (es recomendable identificar todos los orígenes de las amenazas tanto accidentales como deliberadas). Las amenazas se deberían identificar genéricamente y por tipo. Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diversos impactos, dependiendo de los activos que se vean afectados.

A continuación, se exhibe un listado con las amenazas más comunes, retomadas del documento *Guía de Gestión de Riesgos*[16], perteneciente a la serie de Guías enfocadas a la privacidad y seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia[17].

[16] https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf

[17] https://gobiernodigital.mintic.gov.co/portal/Categor-as/Seguridad-y-Privacidad-de-la-Informacion/150516:Guia-7-Gestion-de-Riesgos.pdf

Ellas son:

- Deliberadas;
- Ambientales;
- Accidentales.

Tipo	*Amenaza*	*Origen*
Daño físico	Fuego accidental	Deliberado, Ambiental
	Daños por agua	Accidental, Deliberado, Ambiental
	Contaminación accidental	Deliberado, Ambiental
	Accidente grave	Accidental, Deliberado, Ambiental
	Destrucción de equipos o medios	Accidental, Deliberado, Ambiental
	Polvo, corrosión, congelación	Accidental, Deliberado, 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	Deliberado, Ambiental
	Pérdida de suministro de energía	Accidental, Deliberado, Ambiental
	Fallo del equipo de telecomunicaciones	Deliberado, Ambiental
Perturbación debido a radiación	Radiación electromagnética	Accidental, Deliberado, Ambiental
	Radiación termal	Accidental, Deliberado, Ambiental
	Pulsos electromagnéticos	Accidental, Deliberado, Ambiental
Información comprometida	Intercepción de señales de interferencia comprometedoras	Deliberado
	Espionaje remoto	Deliberado
	Escuchar deliberadamente a escondidas	Deliberado
	Robo de soportes o documentos	Deliberado
	Robo de equipo	Deliberado
	Recuperación de medios reciclados o desechados	Deliberado
	Divulgación	Deliberado
	Datos de fuentes no confiables	Deliberado, Ambiental
	Manipulación de *hardware*	Deliberado
	Manipulación de *software*	Deliberado, Ambiental
	Detección de posición	Deliberado

Tipo	*Amenaza*	*Origen*
Fallas técnicas	Falla en el equipo	Ambiental
	Mal funcionamiento del equipo	Ambiental
	Saturación del sistema de información	Deliberado, Ambiental
	Mal funcionamiento del software	Ambiental
	Incumplimiento del mantenimiento del sistema de información	Deliberado, Ambiental
Acciones no autorizadas	Uso no autorizado de equipos	Deliberado
	Copia fraudulenta de software	Deliberado
	Uso de software falsificado o copiado	Deliberado, Ambiental
	Corrupción de datos	Deliberado
	Tratamiento ilegal de datos	Deliberado
Compromiso de funciones	Error en uso	Ambiental
	Abuso de derechos	Deliberado, Ambiental
	Forja de derechos	Deliberado
	Negación de acciones	Deliberado
	Incumplimiento de disponibilidad de personal	Accidental, Deliberado, Ambiental

Tabla 3. Elaboración propia.

Adicionalmente, puede consultar el árbol de amenazas de la Agencia de la Unión Europea para la Ciberseguridad, ENISA[18].

En caso de requerir mayores elementos sobre las amenazas, puede consultarse el catálogo de amenazas de la metodología MAGERIT[19], que facilita el trabajo de identificación de los activos que puede vulnerar cada amenaza, así como las propiedades o dimensiones que se ven afectadas por la amenaza.

5.4.12. [A.14] Interceptación de información (escucha)

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. **Ver:** EBIOS: 19 - ESCUCHA PASIVA	

5.4.13. [A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

Ejemplo de identificación de amenazas, según MAGERIT.

[18] Para su consulta: https://www.enisa.europa.eu/publications/smart-airports/wp2016-1-1-3-threat-taxonomy.pdf

[19] Para su consulta: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

Ejemplo:

Continuando con el ejemplo anterior, identificando a los currícula vitae como activo, puede realizarse la siguiente identificación de amenazas:

Activo	Valor del activo por dimensión			Valor total cuantitativo	Valor total cualitativo	Amenazas
	C	I	D			
Currículum Vitae en papel: Nombre completo, dirección particular, teléfono particular, experiencia laboral, historia académica.	3	2	1	6	Medio	Fuego (deliberada o ambiental) Fenómeno sísmico (ambiental) Robo de documentos (deliberada) Divulgación de información (deliberada) Daños por agua (accidental, deliberada o ambiental)

Tabla 4. Elaboración propia.

Identificar vulnerabilidades

Las vulnerabilidades son debilidades en la seguridad de los activos. Pueden ser identificadas en los siguientes ámbitos:

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

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

vulnerabilidades. Un control puede ser entonces efectivo o no efectivo, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas con 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 de que un empleado envíe información confidencial a su cuenta personal.

A continuación, se presenta el ejemplo obtenido de la web oficial de la norma ISO 27001 en España[20], y se proponen otros.

Ejemplo:

Activo	*Ejemplo de vulnerabilidad*	*Amenaza*
Documentos en papel. Currículum vitae en papel.	El papel es susceptible de quemarse fácilmente.	Incendio.
Documentos en papel. Currículum vitae en papel.	Los papeles pueden almacenarse en archiveros sin ningún tipo de protección.	Acceso no autorizado, robo o divulgación.
Documentos en papel. Currículum vitae en papel.	Susceptibles al polvo, humedad y deterioro.	Polvo, ambiente que presenta humedad e inundación.
Documentos en papel. Currículum vitae en papel.	Susceptibles de almacenarse sin protección.	Acceso no autorizado por el personal interno. Divulgación por parte de personal interno. Robo de información por personas internas o externas a la entidad.

Tabla 5. Elaboración propia.

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

Estimar el riesgo

Para realizar la estimación o cálculo del riesgo, se recomienda utilizar una escala cuantitativa y su equivalencia cualitativa con atributos calificativos. Esto para describir la magnitud de los impactos o consecuencias potenciales y la probabilidad o posibilidad de

[20] https://normaiso27001.es/asociar-y-documentar-riesgos-amenazas-y-vulnerabilidades-en-iso-27001/. Consultado el 28/01/2022.

que ocurran. La estimación del impacto y probabilidad será realizada por los propietarios de los riesgos.

Ahora bien, el análisis de los riesgos de forma cuantitativa y cualitativa debe realizarse conforme a la fórmula universal del riesgo, donde:

Riesgo= probabilidad x impacto

Recapitulando, tenemos la identificación de activos y su valoración. Posteriormente, por cada activo se habrán identificado sus vulnerabilidades y las amenazas. Por cada activo se asignarán varias amenazas (se recomienda limitar, máximo, a cinco; por ejemplo, priorizando las más importantes), y posteriormente por cada activo-amenaza-vulnerabilidad debe identificarse su impacto y probabilidad. Esto con los criterios que se proponen a continuación.

Criterio para calcular el impacto

El impacto, y por tanto el riesgo, tratándose de un análisis de riesgo de la información, se valora en términos del costo derivado del valor de los activos afectados. Esto considerando, además de los daños producidos en el propio activo, lo siguiente:

I. Daños personales;
II. Pérdidas financieras;
III. Interrupción de servicios;
IV. Daño a la reputación.

Lo anterior puede utilizarse como referencia y no como regla general. En el caso del análisis de riesgos **relativo a los datos personales como activo, y en el sentido de que el derecho a la protección de datos personales se trata de un derecho fundamental, el impacto debe analizarse respecto a los daños o afectaciones a las personas titulares de datos personales**, y no así la afectación a la organización o al sujeto obligado, en sus recursos y su reputación. Si bien esto importa y afecta, no es el fin último y propósito del *Documento de seguridad* y de un Sistema de Gestión de Seguridad de los Datos Personales, en tanto que éstos representan el deber de seguridad que tienen los sujetos obligados de proteger de riesgos y amenazas, en primera instancia, a las personas titulares de datos personales.

Si bien debe valorarse el impacto en el activo, en primer lugar, también debe valorarse respecto al artículo 38 de la *Ley General* a través de un escenario de vulneración, que implica:

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.

La estimación del grado de impacto o consecuencias debe ser determinado mediante la aplicación de criterios en función de los tres principios básicos de seguridad de la información:

- 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.

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

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

Para mayor claridad, se propone el siguiente ejemplo:

Tanto el impacto como la probabilidad deberán tener la misma escala o rango cuantitativo. En este caso se valorará en 5 escalas; donde 1 será un impacto poco significativo o muy bajo, 2 será menor o bajo, 3 será medio, 4 será grave o alto y 5 muy grave o muy alto.

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

Finalmente, el promedio dará el valor numérico total y se traducirá del siguiente modo:

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

Tabla 6. Elaboración propia.

Ejemplo:

Activo	*Amenaza*	*Impacto*			
Currículum vitae		C	I	D	Impacto inherente total
	Incendio	1-Muy bajo	1-Muy bajo	2-Bajo	1.3=1-Muy bajo
	Robo de documentos	3-medio	3-medio	2-bajo	2.6= 3-Medio

Tabla 7. Elaboración propia.

Criterio para calcular la probabilidad

Se refiere a la posibilidad de que un evento ocurra, considerando la cantidad de veces que podría presentarse en determinado período, basándose en las eventualidades conocidas y el conocimiento del entorno, o bien a través de juicio de una persona experta. Se proponen las siguientes escalas:

Grado de Probabilidad		*Criterio*
Muy baja	*1*	No existe antecedente registrado en los últimos 10 años, y/o que por el entorno la posibilidad de que suceda sea mínima.
Baja	*2*	Ha ocurrido un antecedente registrado en un período de 5 años, o que por el entorno y condiciones sea posible que ocurra.
Media	*3*	Se ha presentado un antecedente registrado en un período anual y/o esporádicamente en intervalos de 3 a 5 años, o que por el tipo de entorno y condiciones sea posible que ocurra.
Alta	*4*	Han ocurrido más de dos eventos al término de un año, o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.
Muy Alta	*5*	Se ha presentado un evento en más de dos ocasiones en un período anual, y por las condiciones actuales o el tipo de entorno es muy probable que ocurran constantemente, quizá una vez al mes.

Tabla 8. Elaboración propia.

Ejemplo:

Activo	*Amenazas*	*Probabilidad*
Currículum Vitae	Incendio	1-Muy baja Justificación: en tanto que no hay registro en los últimos de incendio en 10 años.
	Robo de información	4-Alta Justificación: Se tiene registrado que ha habido 2 robos de información en la entidad en el último año.

Tabla 9. Elaboración propia.

La justificación no será necesaria. En el caso del ejemplo, se ha realizado para razonar la decisión del rango cuantitativo.

Determinación del nivel de riesgo

El nivel de riesgo debe ser representado en una escala cuantitativa y cualitativa. Para este documento se recomienda una escala de 5 niveles en orden creciente y su equivalencia cuantitativa (1, 2, 3, 4 y 5), respectivamente. Ahí 1 será riesgo muy bajo; 2, bajo; 3, medio; 4, alto y 5 muy alto. Para su determinación, como se mencionó, se deberá multiplicar el valor final del impacto por la probabilidad.

Importante

En este paso, para valorar el riesgo inherente, la estimación del impacto y la probabilidad, debe realizarse sin considerar ningún control o medida de seguridad implantada en el sujeto obligado por mínima que sea. Dentro del análisis de brecha, se considerarán las medidas de seguridad ya impuestas y las que se implementarán, pudiendo así calcular el riesgo residual.

- Los valores 1-2 (muy bajo) serán riesgos aceptables.
- Los valores 3-4 (bajo) serán riesgos aceptables. No deberán ser tratados, pero sí monitoreados.
- Los valores 5- 9 (medio) serán riesgos no aceptables. Deberán ser tratados.
- Los valores 10-19 (alto) son riesgos no aceptables. Deberá priorizarse el tratamiento del riesgo para aquellos activos de mayor a menor valor; 3 (alto), 2 (medio) y 1 (bajo).
- Los valores 20-25 (muy alto) son riesgos no aceptables. Serán a los que se les dará prioridad en el tratamiento del riesgo.

Para facilitar la visualización, se presenta esta matriz de riesgos o mapa de calor:

PROBABILIDAD	Insignificante = 1	Menor = 2	Crítico = 3	Grave = 4	Muy grave = 5
Muy alta = 5	5	10	15	20	25
Alta = 4	4	8	12	16	20
Media = 3	3	6	9	12	15
Baja = 2	2	4	6	8	10
Muy baja = 1	1	2	3	4	5
			IMPACTO		

Tabla 10. Elaboración propia.

De este modo, 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	Muy alto	2	Baja	10	Alto
5	Muy alto	3	Media	15	Alto
5	Muy alto	4	Alta	20	Muy alto
5	Muy alto	5	Muy alta	25	Muy alto
4	Alto	1	Muy baja	4	Bajo
4	Alto	2	Baja	8	Medio
4	Alto	3	Media	12	Alto
4	Alto	4	Alta	16	Alto
4	Alto	5	Muy alta	20	Muy alto
3	Medio	1	Muy baja	3	Bajo
3	Medio	2	Baja	6	Medio
3	Medio	3	Media	9	Medio
3	Medio	4	Alta	12	Alto
3	Medio	5	Muy alta	15	Alto
2	Bajo	1	Muy baja	2	Muy bajo
2	Bajo	2	Baja	4	Bajo
2	Bajo	3	Media	6	Medio
2	Bajo	4	Alta	8	Medio
2	Bajo	5	Muy alta	10	Alto
1	Muy bajo	1	Muy baja	1	Muy bajo
1	Muy bajo	2	Baja	2	Muy bajo
1	Muy bajo	3	Media	3	Bajo
1	Muy bajo	4	Alta	4	Bajo
1	Muy bajo	5	Muy alta	5	Medio

Tabla 11. Elaboración propia.

Ejemplo:

Activo	*Amenaza*	*Impacto*				*Probabilidad*	*Riesgo inherente*
Currículum vitae		*C*	*I*	*D*	*Impacto total*		
	Incendio	1	1	2	1.3= 1-Muy bajo	1-Muy baja	1-Muy bajo
	Robo de documentos	3	3	2	2.6= 3-Medio	4-Alta	12= Alto

Tabla 12. Elaboración propia.

Como muestra el ejemplo, deberá priorizarse el tratamiento del riesgo de robo de documentos, en este caso del currículum, en tanto que hay un alto riesgo. Eso contrario al riesgo de incendio, que es mínimo.

Identificar Escenarios de vulneración y Consecuencias para los titulares

Una vez que se ha identificado las amenazas y las vulnerabilidades a las que se enfrentan los activos, y ya que realizó una valoración del impacto, la probabilidad y el nivel de riesgo inherente, es necesario que se incluyan todos los hallazgos en una tabla que permita asociar e identificar claramente las consecuencias y los perjuicios que se causarían a los titulares, de materializarse el riesgo en los activos, como, por ejemplo, sin ser éste 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.

El sujeto obligado debe, una vez valorado el riesgo para el activo, estimar las consecuencias en los titulares, de materializarse dicho riesgo.

Ejemplo:

Activo	*Amenaza*	*Vulnerabilidad*	*Impacto*				*Probabilidad*	*Riesgo inherente*
			C	*I*	*D*	*Impacto total*	*Probabilidad*	
Currículum vitae	Incendio	Susceptible de quemarse	1	1	2	1.3= 1 Muy bajo	1-Muy baja	1-Muy bajo
	Robo de documentos	Almacenamiento sin protección	3	3	2	3.2= 3 Medio	4-Alta	12-Alto
Análisis de impacto para los titulares								
De materializarse el riesgo «incendio», no se considera que haya un impacto directo sobre los titulares, salvo molestias en caso de tener que solicitarlos nuevamente. De materializarse el riesgo «robo de documentos», los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad, en tanto que el CV contiene su dirección y teléfono particulares; • Pérdida de control de sus datos personales; • Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral. • En este caso, el riesgo que debe priorizarse para proteger a los titulares es el de «robo de documentos».								

Tabla 13. Elaboración propia.

Una vez realizado este análisis, se deberá pasar al análisis de brecha. Es decir, el análisis de los controles o medidas de seguridad.

ETAPA 4

EL ANÁLISIS DE BRECHA

Es el cuarto rubro del *Documento de seguridad*. Consiste en identificar la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales. Puede definirse como la concentración de elementos específicos que pueden existir entre lo deseable y lo actual. Para ello es importante definir con claridad cuál es la brecha que se desea analizar, identificar quiénes están involucrados, establecer cuáles son las causas más relevantes que determinan la brecha, identificar las diferencias de comportamiento entre los sistemas o actores a comparar en la brecha, identificar los indicadores y/o atributos de la situación actual y elaborar un listado para medir o caracterizar la brecha.[21]

En este paso es necesario tomar una decisión sobre las actividades a realizar, para tratar los riesgos identificados en la etapa anterior.

Debe entenderse que la gestión del riesgo es el proceso de conocerlo y comprenderlo para tratarlo adecuadamente, para decidir sobre la opción de tratamiento idóneo y que más convenga al sujeto obligado. El tratamiento de los riesgos implica identificar el rango de opciones con miras a ocuparse de los riesgos, evaluar esas opciones y preparar planes para dicho tratamiento e implementarlos.

El análisis de brecha como contenido del *Documento de seguridad*, en relación con un Sistema de Gestión de Seguridad de Datos Personales, es la etapa del tratamiento del riesgo en sentido estricto, ya que es cuando debe decidirse qué hacer con el nivel de riesgo detectado.

En ese sentido, los controles pueden proporcionar diversas opciones de tratamiento de riesgo:

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

[21] INAI y Davara F. de Marcos (2019, noviembre), *Diccionario de Protección de Datos Personales*. Fecha de consulta: 22 de marzo de 2022. Disponible en:http://inicio.ifai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

controles contra el valor del activo a proteger. Adicionalmente, debe tenerse 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 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 entrenamiento establecido con la debida anterioridad, llevando a los usuarios a escribir las contraseñas en papel. Los responsables deben identificar las soluciones que satisfagan sus requerimientos y garanticen suficiente seguridad de los datos personales.

Retener el riesgo

Significa retener la responsabilidad por las pérdidas de los activos debido a 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 los titulares de los datos personales, en tanto se busca implementar otra opción de tratamiento del riesgo.

Puede decidirse retener el riesgo sin considerar medidas adicionales, si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles pueden implementarse posteriormente. Por ejemplo, el equipo de cómputo actual falla, pero al final del día se genera un respaldo de esa información; por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

Evitar el riesgo

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, retirándose de las actividades actuales o cambiando las condiciones bajo las cuales operan dichas actividades. Por ejemplo, para un riesgo causado por la naturaleza podría ser más eficiente en costo mover físicamente el *site* de datos a una ubicación donde no exista el mismo riesgo, o que pueda mantenerse bajo control.

Compartir el riesgo

Implica tomar la decisión de compartir el riesgo con un prestador de servicio que pueda gestionarlo. Es decir, un tercero interviene para mitigar los posibles efectos de un riesgo.

Por ejemplo, al contratar un seguro o un proveedor que administre la seguridad del sujeto obligado.

En algunas ocasiones, las organizaciones deciden contratar seguros contra riesgos. De este modo, el riesgo se traslada a la entidad asegurada. Cabe mencionar que, 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 afecte a los datos personales, será el sujeto obligado quien debe responder. 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 se decide aceptar las consecuencias y probabilidad de un riesgo en particular.

Esta opción se toma cuando los costos de implementación de una medida de seguridad sobrepasan el valor del activo que se desea proteger, o cuando el nivel del riesgo es muy bajo. En ambos casos, la organización asume los daños provocados por la materialización del riesgo. En materia de seguridad enfocado a datos personales, debemos recordar que no sólo debe considerarse el valor del activo, sino también el impacto que puede causar su daño o pérdida a los titulares de los datos personales.

Dentro de la Organización para la implementación del SGSDP, durante la planeación deben establecerse criterios para la gestión del riesgo dentro de los cuales está el Nivel de Riesgo Aceptable. Como se indicó en el punto 3 del apartado «Definición del alcance, contexto y objetivos del análisis de riesgos», se recomienda que sea bajo o muy bajo. Ahora bien, dentro del tratamiento del riesgo, la entidad deberá ceñirse a lo establecido en dicho criterio. Aunque es posible que, por causas como la falta de recursos económicos, administrativo o humanos, deba aceptarse un riesgo de mayor nivel, lo cual se recomienda sea excepcional. En ese caso, será importante que se documente y sea aprobado por la o las personas propietarias del tratamiento, por el Comité de Transparencia y de ser posible por los Órganos Directivos de la entidad, a efecto de que el responsable del tratamiento esté aceptando un riesgo distinto al establecido en los criterios para la gestión del riesgo.

Finalmente, para efectos de la comprensión del riesgo, es importante aclarar 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, deben considerarse los riesgos que es casi imposible que ocurran pero que serían catastróficos de suceder, en cuyo caso también deben implementarse controles de monitoreo y vigilancia. A éstos se les denomina en teoría «cisne

negro»[22], debido a que la probabilidad de que sucedan es remota pero, de suceder, serían fatales en cuanto al impacto.

Ahora bien, los cuatro tipos de tratamiento de riesgo no son mutuamente excluyentes. A veces, los sujetos obligados pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual.

Comunicación del riesgo

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

Importante

La comunicación efectiva entre los involucrados es muy importante, pues impacta en las decisiones que deban tomarse respecto a la gestión del riesgo. De ahí que tendría que ser bidireccional, para asegurar que los involucrados en la elaboración del *Documento de seguridad*, en la implementación del SGSDP y las partes interesadas entiendan los criterios en los que se basan las decisiones.

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

La comunicación del riesgo debe realizarse para alcanzar los siguientes objetivos:

- Ofrecer garantías sobre la gestión del riesgo en el sujeto obligado;
- 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 sobre el riesgo;
- Incrementar la conciencia del riesgo en la organización.

La coordinación entre las personas principales que toman 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. Esto 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 éstas conllevan, como la notificación a los titulares y, en su caso, al Instituto y los Organismos garantes.

Artículo 40 de la *Ley General*:

«El responsable deberá informar sin dilación alguna al titular y, según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.».

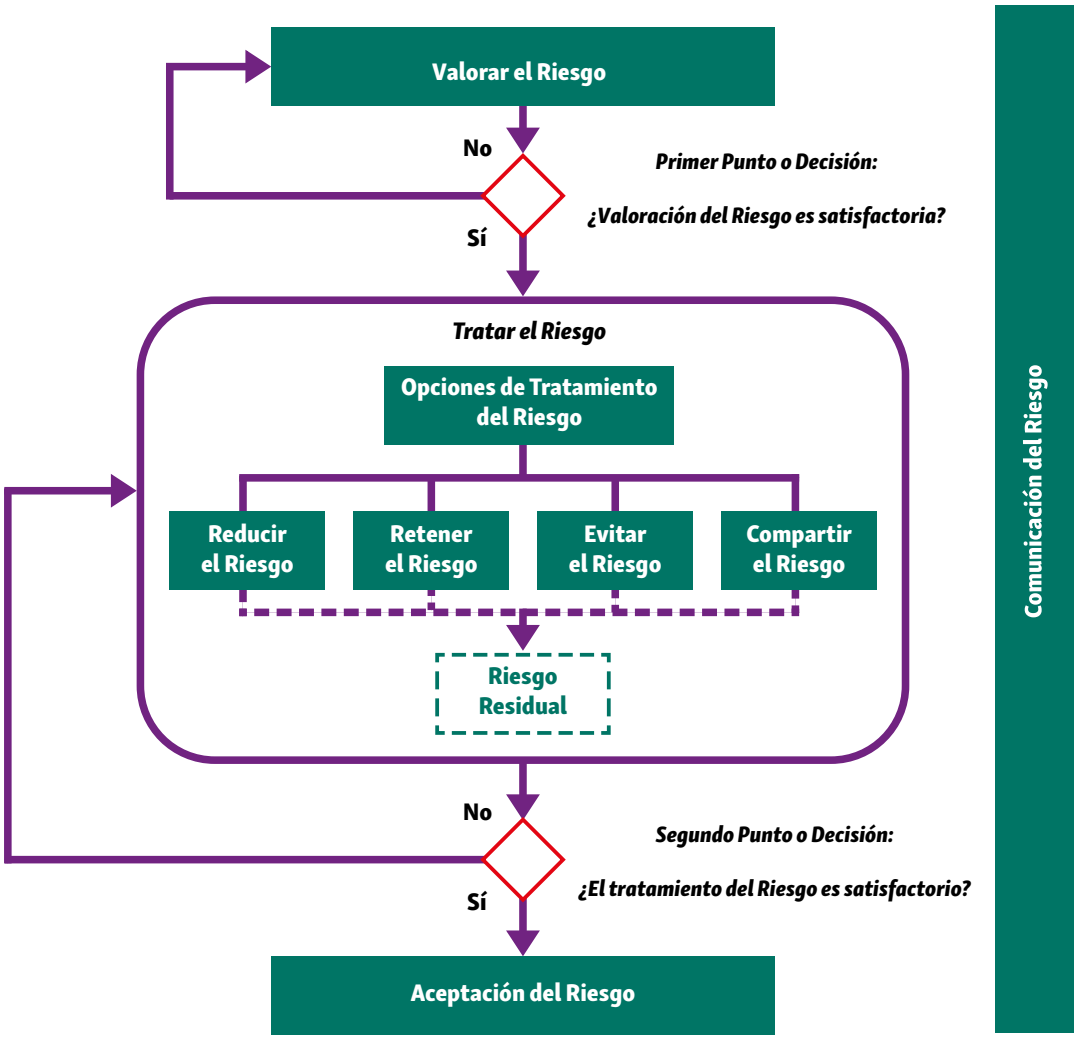


Figura 6. Tratamiento del Riesgo[23].

Entender las opciones de tratamiento de riesgo, así como la comunicación, hará más claro entender el análisis de brecha. Esto porque seleccionar las opciones de tratamiento de riesgo correspondientes conlleva determinar las medidas o controles de seguridad que materialicen dicha opción. Por ejemplo, si lo que se elige es reducir el riesgo para un activo en particular, deben analizarse los controles existentes, evaluar si éstos funcionan o pueden fortalecerse, o si deben implementarse otros y, una vez que se ha definido el tratamiento del riesgo y las medidas de seguridad a implementar, se requiere determinar el riesgo residual. Si éste no cubre los niveles de aceptación del sujeto obligado,

[23] INAI (2015, junio) *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, p. 25. Fecha de consulta: 09/05/2022. Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

deberá realizarse otra iteración de tratamiento del riesgo con nuevas o distintas medidas de seguridad, hasta que se obtenga un nivel de riesgo aceptable.

Para el análisis de brecha será imprescindible contar con la colaboración de los titulares de área, con miras a hacer un análisis de las medidas implementadas y de las que pueden implementarse según las posibilidades reales de la unidad administrativa: esto es, los recursos humanos, administrativos y los presupuestos con los que cuenta el área.

En ese orden, la *Ley General* establece que los sujetos obligados deberán observar:

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. [...]

IV. [...]

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;»

Artículo 61 de los *Lineamientos Generales*:

«**El Análisis de brecha**

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.»

Para una mejor implementación e identificación de las medidas de seguridad, es recomendable que los principios establecidos en el artículo 16 de la *Ley General* se utilicen como base para la selección de medidas de seguridad, y de este modo se encuentren alineadas a la protección de datos personales. En particular, pueden considerarse los siguientes criterios para elegir las medidas de seguridad efectivas que:

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

Una vez identificados los activos y procesos relacionados con los datos personales, así como las amenazas, vulnerabilidades y escenarios de vulneración relacionados, se puede iniciar con el análisis de brecha de las medidas de seguridad.

Como lo indica la *Ley General*, el análisis de brecha consiste en identificar:

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

Con base en el análisis de riesgos, se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas que permitan disminuir los riesgos, en algunos casos como el que se expone. Se considera viable que, además de tomar en cuenta las medidas de seguridad implementadas al interior del sujeto obligado, y en caso de requerir alguna referencia adicional, se considere por ejemplo el catálogo de controles de seguridad identificados en la norma ISO/IEC 27001:2013, o el de la metodología MAGERIT 3.0[24].

Al hablar de una comparativa respecto a controles existentes y faltantes, se sugiere primero identificar los controles de seguridad implementados en cada área, documentarlos, analizarlos y valorarlos. Pero, si posterior a ello se busca fortalecer estas acciones de seguridad, una buena medida es identificar en la metodología adoptada la existencia de otros controles.

Debe consignarse que no todos los controles pueden aplicar a su sistema de tratamiento de información, pues algunos pueden ser no compatibles con el tipo de sistema en que se encuentra la información.

Para el análisis de los controles o medidas de seguridad, es necesario precisar que éstas tienen distintas categorías según su función. Algunas son:

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

- Correctivas;
- Preventivas;
- Disuasorias;
- Detectivas.

Para determinar las medidas de seguridad, será importante categorizarlas a efecto de que sea más sencillo el análisis posterior para la reducción del riesgo. Esto es así, ya que debe considerarse que algunas medidas de seguridad reducen el impacto y otras la probabilidad, por lo que habrá que analizarlas a fondo para advertir si realmente éstas reducen el riesgo objetivamente. Por ejemplo, la medida de seguridad consistente en control de accesos físicos es una medida por su naturaleza de prevención 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 al atacante a cambiar de opinión o a desistir de un propósito. Por ello, esta medida reduce la probabilidad de ocurrencia; pero, de materializarse el riesgo, aunque tengamos control de accesos, no reduciría el impacto en los activos ni en los titulares de los datos personales afectados.

Asimismo, es recomendable analizar el nivel de madurez en su implementación y funcionamiento. Parte fundamental del análisis de brecha es estudiar si las medidas de seguridad requieren fortalecerse, o bien implementar alguna otra que la complemente para proteger adecuadamente el activo analizado.

En la elaboración del análisis de brecha, puede utilizarse como referencia la tabla de controles de seguridad contenida en el Anexo D de la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015*.

A continuación se muestra el catálogo de salvaguardas de la metodología MAGERIT v.3., y una referencia sobre los contenidos del catálogo de la ISO/IEC/27002.

MAGERIT V.3

«6. Salvaguardas

6.1. Protecciones generales u horizontales

H Protecciones Generales
H.IA Identificación y autenticación
H.AC Control de acceso lógico
H.ST Segregación de tareas
H.IR Gestión de incidencias
H.tools Herramientas de seguridad
H.tools.AV Herramienta contra código dañino
H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión

H.tools.CC Herramienta de chequeo de configuración
H.tools.VA Herramienta de análisis de vulnerabilidades
H.tools.TM Herramienta de monitorización de tráfico
H.tools.DLP DLP: Herramienta de monitorización de contenidos
H.tools.LA Herramienta para análisis de logs
H.tools.HP Honey net / honey pot
H.tools.SFV Verificación de las funciones de seguridad
H. VM Gestión de vulnerabilidades
H. AU Registro y Auditoría

6.2. Protección de los datos / información

D Protección de la Información
D.A Copias de seguridad de los datos (backup)
D.I Aseguramiento de la integridad
D.C Cifrado de la información
D.DS Uso de firmas electrónicas
D.TS Uso de servicios de fechado electrónico (time stamping)

6.3. Protección de las claves criptográficas

K Gestión de claves criptográficas
K.IC Gestión de claves de cifra de información
K.DS Gestión de claves de firma de información
K.disk Gestión de claves para contenedores criptográficos
K.comms Gestión de claves de comunicaciones
K.509 Gestión de certificado

6.4. Protección de los servicios

S Protección de los Servicios
S.A Aseguramiento de la disponibilidad
S.start Aceptación y puesta en operación
S.SC Se aplican perfiles de seguridad
S.op Explotación
S.CM Gestión de cambios (mejoras y sustituciones)
S.end Terminación
S.www Protección de servicios y aplicaciones web
S.email Protección del correo electrónico
S.dir Protección del directorio
S.dns Protección del servidor de nombres de dominio (DNS)
S.TW Teletrabajo
S.voip Voz sobre IP

6.5. Protección de las aplicaciones (*software*)

SW Protección de las Aplicaciones Informáticas
SW.A Copias de seguridad (backup)
SW.start Puesta en producción
SW.SC se aplican perfiles de seguridad
SW.op Explotación/producción
SW.CM Cambios (actualización y mantenimiento)
SW.end Terminación

6.6. Protección de los equipos (*hardware*)

HW Protección de los Equipos Informáticos
HW.start Puesta en producción
HW.SC Se aplican perfiles de seguridad
HW.A Aseguramiento de la disponibilidad
HW.op Operación
HW.CM Cambios (actualizaciones y mantenimiento)
HW.end Terminación
HW.PCD Informática móvil
HW.print Reproducción de documentos
HW.pabx Protección de la centralita telefónica

6.7. Protección de las comunicaciones

COM Protección de las comunicaciones
COM.start Entrada de servicio
COM.SC Se aplican perfiles de seguridad
COM.A Aseguramiento de disponibilidad
COM.aut Autenticación del canal
COM.Iprotección de la integridad de los datos intercambiados
COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
COM. Op Operación
COM.CM Cambios (actualizaciones y mantenimiento)
COM.end Terminación
COM.Internet: uso de acceso
COM.wifi Seguridad wireless (WiFi)
COM.Mobile Telefonía móvil
COM.DS Segregación de las redes en dominios

6.8. Protección en los puntos de interconexión con otros sistemas

IP Puntos de interconexión: conexiones entre zonas de confianza
IP SPP Sistema de protección perimetral
IP.BS Protección de los equipos de frontera

6.9. Protección de los soportes de información

MP Protección de los soportes de información
MP.A Aseguramiento de la disponibilidad
MP.IC Protección criptográfica del contenido
MP.clean Limpieza de contenidos
MP.end Destrucción de soportes

6.10 Protección de los elementos auxiliares

AUX Elementos auxiliares
AUX.A Aseguramiento de la disponibilidad
AUX.start Instalación
AUX.power Suministro eléctrico
AUX A.C. Climatización
AUX.wires Protección de cableado

6.11 Seguridad física-Protección de las instalaciones

L Protección de las instalaciones
L.design Diseño
L.depth Defensa en profundidad
L.AC Control de los accesos físicos
L.A Aseguramiento de la disponibilidad
L.end Terminación

6.12 Salvaguardas relativas al personal

PS Gestión del personal
PS.AT Formación y concienciación
PS.A Aseguramiento de la disponibilidad

6.13 Salvaguardas de tipo organizativo

G Organización
G.RM Gestión de riesgos
G. plan Planificación de la seguridad
G.exam Inspección de seguridad

6.14. Continuidad de operaciones (Prevención y reacción frente a desastres)

BC Continuidad del negocio
BC.BIA Análisis de Impacto
BC.DRP Plan de Recuperación de Desastres (DRP)

6.15 Externalización

SLA: nivel de servicio
NDA: (non disclosure agreement) compromiso de secreto
Identificación y calificación del personal encargado
Procedimientos de escalado y resolución de incidencias
Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)
Asunción de responsabilidades y penalizaciones por incumplimiento

E Relaciones externas

E.1 Acuerdos de intercambio para información y software
E.2 Acceso externo
E.3 Servicios proporcionados por otras organizaciones
E.4 Personal subcontratado

6.16 Adquisiciones y desarrollo

NEW Adquisición/desarrollo
NEW.S Servicio: adquisición o desarrollo
NEW.SW: Aplicaciones: adquisición o desarrollo
NEW.HW Equipos: Adquisición o desarrollo
NEW.COM Comunicaciones: Adquisición o contratación
NEW.C Productos certificados o acreditados.»[25]

[25] Ministerio de Hacienda y Administraciones Públicas, *Metodología de análisis y gestión de riesgos de los Sistemas de Información*, Magerit v3, Libro II-catálogo de elementos (2012), Madrid. Disponible en: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file. Consultado el 13-06-2022.

ISO 27002

Políticas de seguridad de la información

Dirección de gestión para la seguridad de la información (2 controles)

1. Organización de la seguridad de la información
    1. Organización interna (5 controles)
    2. Dispositivos móviles y teletrabajo (2 controles)
2. Seguridad de los recursos humanos
    1. Antes del empleo (2 controles)
    2. Durante el empleo (3 controles)
    3. Terminación y cambio de empleo (1 control)
3. Gestión de archivos
    1. Responsabilidad por activos (4 controles)
    2. Clasificación de la información (3 controles)
    3. Manejo de medios (3 controles)
4. Control de acceso
    1. Requisitos comerciales de control de acceso (2 controles)
    2. Gestión de acceso a usuarios (6 controles)
    3. Responsabilidades del usuario (1 control)
    4. Control de acceso a sistemas y aplicaciones (5 controles)
5. Criptografía
    1. Controles criptográficos (2 controles)
6. Seguridad física y ambiental
    1. Áreas seguras (6 controles)
    2. Equipo (9 controles)
7. Seguridad de las operaciones
    1. Procedimientos operativos y responsabilidades (4 controles)
    2. Protección contra un programa maligno (*malware*) (1 control)
    3. Copia de seguridad (1 control)
    4. Registro y seguimiento (4 controles)
    5. Control de *software* operativo (1 control)
    6. Gestión de vulnerabilidades técnicas (2 controles)
    7. Consideraciones de auditoría de sistemas de información (1 control)
8. Seguridad de las comunicaciones
    1. Gestión de la seguridad de la red (3 controles)
    2. Transferencia de información (4 controles)
9. Adquisición, desarrollo y mantenimiento de sistemas
    1. Requisitos de seguridad de los sistemas de información (3 controles)
    2. Seguridad en los procesos de desarrollo y soporte (9 controles)

3. Datos de prueba (1 control)

10. Relación con proveedores
    1. Seguridad de la información en las relaciones con los proveedores (3 controles)
    2. Gestión de la prestación de servicios del proveedor (2 controles)
11. Gestión de incidentes de seguridad de la información
    1. Gestión de incidentes y mejoras de seguridad de la información (7 controles)
12. Aspectos de seguridad de la información de la gestión de la continuidad del negocio
    1. Continuidad de la seguridad de la información (3 controles)
    2. Redundancias (1 control)
13. Cumplimiento
    1. Cumplimiento de requisitos legales y contractuales (5 controles)
    2. Revisiones de seguridad de la información (3 controles)

De modo general, para una mejor consulta de los controles de seguridad que se identifican y que pueden formar parte de los resultados del análisis de brecha como controles de seguridad no implementados, se sugiere contar con una tabla que identifique el control, describa de qué se trata y que incluya una breve descripción respecto a las tareas realizadas para hacer evidente el cumplimiento de dicho control. Adicionalmente, para un mejor resultado, es necesario identificar al responsable de operar el control y de quien lo supervisa.

Como se mencionó, es importante tener claro cuáles son los controles que ya están funcionando de manera efectiva en una organización, con su respectivo nivel de madurez. El nivel de madurez de las medidas de seguridad se refiere a la eficacia que tienen frente al riesgo y qué tan correctamente implantadas están en el sujeto obligado.

De acuerdo con la metodología MAGERIT, se considera que una medida de seguridad tiene una eficacia del 0% cuando es inexistente y un 100% aquéllas que están implantadas, que son idóneas, medibles, existen procedimientos claros de uso normal y, en caso de incidencias, los usuarios están formados y concienciados en torno a que existen controles que avisan de posibles fallos.

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

Factor	*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.
	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 14. Escala obtenida del Libro I de Magerit V.3[26], complementada con criterios propios basados en la metodología.

De acuerdo con la escala anterior, se propone que el sujeto obligado realice una tabla con los activos, la amenaza, el riesgo inherente y la columna de control o medida ya implementada, evidencia del cumplimiento del control, el responsable de la medida, así como su respectivo nivel de madurez.

Ejemplo:

Siguiendo con el ejemplo del currículum vitae utilizado para el análisis de riesgos, supongamos ahora que sólo nos referimos a los CV en físico (por tanto, a la amenaza de robo de información en físico), y que el sujeto obligado cuenta con una medida de seguridad que realiza de vez en cuando: solicitar que quienes ingresarán a la gaveta o archivero donde se encuentran los documentos en físico se registren en una bitácora. Se tendría que analizar el control de seguridad por su naturaleza y si éste disminuye el riesgo; además del nivel de madurez de su implementación respecto a lo establecido anteriormente.

[26] Ministerio de Hacienda y Administraciones Públicas, *Metodología de análisis y gestión de riesgos de los Sistemas de Información, Magerit v3, Libro I-Método* (2012), Madrid. Disponible en: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file. Consultado el 13-06-2022 P.34

Activo	*Amenaza*	*Riesgo inherente*						*Control (es) de seguridad implantado (os)*	*Evidencia*	*Responsable*	*Nivel de madurez*
		Impacto				*Probabilidad*	*Riesgo*				
		C	*I*	*D*	*IT*						
CV en papel	Robo de documentos (físico)	3	3	2	3 Medio	4 Alta	12 Alto	1.Control de accesos físicos. Se ha solicitado que las personas que requieran consultar los CV en físico se registren en bitácora. Medida física, preventiva y disuasoria.	1. Se mantiene una libreta donde se solicita nombre y firma de quien abre el archivero y debe mencionar qué CV consulta, así como la hora en que lo devuelve.	Titular del departamento de contratación	L2- Hay una persona que la impulsó de forma preventiva y constante, de acuerdo con su criterio; pero no está documentada.

Tabla 15. Elaboración propia.

Una vez realizado lo anterior, se recomienda analizar si el control implementado realmente reduce el nivel de riesgo. Para ello es importante retomar el procedimiento de análisis de riesgos y valorar si el control implementado reduce el impacto en alguna de las dimensiones (CID) o la probabilidad. A partir de ello puede volver a valorarse el riesgo con la fórmula riesgo= probabilidad x impacto.

Para efectos del ejemplo, tendríamos que preguntarnos cuál es la categoría de la medida y su función o naturaleza. En este caso, es una medida física, en tanto que evita el acceso físico al activo. Es preventiva, en tanto que se impuso para efectos de prevenir accesos y el robo de la información. Es disuasoria, ya que el personal, al saber que se debe registrar en una bitácora, pone más atención en no perder el archivo y cuidarlo, pues se ejerce cierto nivel de vigilancia sobre ellos. En ese sentido, puede observarse que la medida reduce la probabilidad de que se materialice la amenaza. En cambio, aunque exista esta medida, si llegasen a robar la información, ésta no reduce el impacto en el activo ni en la persona titular de los datos personales.

En ese sentido, tenemos que:

Control implementado	*Reduce Probabilidad*	*Reduce impacto*	*Riesgo actual*
Control de accesos: Se mantiene una bitácora de registro de accesos al archivero.	Si; pasa de 4 a 3 = Media	No= 3-Medio	9= Medio

Tabla 16. Elaboración propia.

En el ejemplo, la medida de control de accesos no reduce por sí sola el riesgo a un nivel bajo. De tener sólo este control, tendría que implementarse una segunda, o bien el sujeto obligado podría decidir aceptar el riesgo, siempre que se firme un acta por el Comité de Transparencia, los titulares de la unidad administrativa y los responsables. No obstante, el hecho de aceptar un riesgo de este nivel no elimina ni reduce la responsabilidad en caso de vulneración, sino incluso puede traer consecuencias por no cumplir con los deberes de seguridad y el principio de responsabilidad.

Es importante considerar que el nivel de madurez es bastante bajo (L2). Es una medida que se está implementando por mera noción de una persona que considera que es correcto hacerlo, sin ser obligatorio dentro de la entidad, y sin estar documentado, por lo que es posible que no se esté cumpliendo ni adecuada ni continuamente. Por ello debería trabajarse para mejorarla y por lo menos llegar a un nivel L-4, es decir, que sea gestionable y medible a fin de poder evaluar su eficacia. En este caso, por ejemplo, podría realizarse una política de control de accesos físicos. Esto es, se añade un control al ser una medida de seguridad administrativa que puede reducir el riesgo; y robustece el control actual para que se vuelva obligatoria y constante, con lo que se aumenta también su madurez.

Ahora bien, supongamos que se decide crear un procedimiento de control de accesos físicos para el tratamiento de Recursos humanos —tratamiento de aspirantes al empleo en particular—, donde se señala que sólo podrán acceder dos personas al archivero donde se encuentran, por lo que únicamente esas dos personas pueden tener las llaves.

Control(es) implementado(os)	*Reduce Probabilidad*	*Reduce impacto*				*Riesgo residual*	*Nivel de madurez de la medida*
		C	*I*	*D*	*IT*		
Control de accesos (bitácora)	Sí; reduce de 4 a 3= media	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	9=Medio	L2
Procedimiento de control de accesos físicos	Sí; reduce de 3 a 2	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	6=Medio	L3
Control de accesos-limitar la entrada a dos personas	Sí; reduce de 2 a 1	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	3=Bajo	L3

Tabla 17. Elaboración propia.

Con el fortalecimiento o robustecimiento de la medida de seguridad con la que ya contaba el sujeto obligado, es posible disminuir el riesgo y a su vez fortalecer el nivel de madurez de la medida. Ahora bien, respecto al análisis de la naturaleza de las medidas, ambas disminuyen la probabilidad pero no el impacto, por lo que sería deseable implementar alguna que disminuyera éste. Por ejemplo, que la entidad tuviera su propio formato de CV *ad hoc*, sin datos personales, a fin de que se reciban y resguarden sólo con la información realmente necesaria, omitiendo teléfonos personales, correos electrónicos y direcciones particulares. De ser así, el impacto podría disminuir en cuanto a la dimensión de confidencialidad, mas no en integridad y disponibilidad; ya que, al asociar el nombre del titular a una historia académica y laboral, aún es posible modificar esta información sin autorización (afectar la integridad) y causar algún daño al titular de los datos personales.

De igual modo, la disponibilidad no se ve afectada en ningún sentido, por lo que sólo reduciría la confidencialidad de 4 a 3 y el impacto total seguiría siendo 3 (reduce a 2.6; sin embargo, para mayor entendimiento, se utilizan cifras cerradas).

Ahora traslademos el ejemplo a un escenario tecnológico. Tenemos una base de datos donde se resguardan los CV en digital con datos personales incluidos dirección postal, correo electrónico particular, teléfonos personales, historia académica y laboral. Dicha base de datos cuenta con un control de accesos donde se ingresa sólo con usuario y contraseña. Además dicho control fue impuesto de facto por el administrador de la base, y no está documentado.

Activo	*Amenaza*	*Riesgo inherente*						*Control (es) de seguridad implantado (s)*	*Evidencia*	*Responsable*	*Nivel de madurez*
		I				*P*	*Riesgo*				
		C	*I*	*D*	*IT*						
CV en digital-base de datos	Filtración de documentos-acceso no autorizado-divulgación.	3	3	2	3-Medio	4-Alta	12-Alto	1. Control de accesos lógico. Para ingresar a la BBDD, debe contar con usuario y contraseña.	1. El área encargada de implementar la medida cuenta con directorio de usuarios.	Subdirector de DGTI	L2- Hay una persona que la impulsó de modo preventivo y constante de acuerdo con su criterio, pero no está documentado.

Tabla 18. Elaboración propia.

Tenemos, entonces, un control de accesos donde se solicita usuario y contraseña para ingresar a los archivos. Sin embargo, dicha medida tiene un nivel de madurez L2-repetible pero intuitivo, en tanto que lo impulsó de facto el responsable de administrar la base de datos.

Control implementado	*Reduce Probabilidad*	*Reduce impacto*	*Riesgo actual*
Control de accesos: usuario y contraseña de usuarios, quienes están registrados en un directorio.	Sí; reduce de 4 a 3= Media	No= 3-Medio	9= Medio

Tabla 19. Elaboración propia.

Supongamos que, al igual que en el ejemplo anterior, implementamos la documentación de un procedimiento de control de accesos lógico. Además, se decide robustecer dicho control con una autenticación de doble factor, donde se limitará el acceso a usuarios registrados y —mediante usuario, contraseña y confirmación por número de seguridad enviado al correo institucional— la información se seudonimiza[27], ya que la base de datos se disocia, por lo que mediante controles técnicos se desvincula la información del CV de su titular, quedando sólo un número de aspirante. Además, al digitalizar el documento se respalda

[27] Seudonimizar. Seudonimización, según el *Reglamento General de Protección de Datos* del Parlamento Europeo y del Consejo de 27 de abril de 2016, se refiere al tratamiento de datos personales, de modo que ya no puedan atribuirse a un interesado (titular) sin utilizar información adicional; siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

en digital en versión pública, eliminando los datos personales que no son necesarios. Por otro lado, existe un responsable de llevar a cabo la medida y ésta es medible mediante indicadores de cumplimiento, lo que sirve en la realización de auditorías para la mejora de la gestión, por lo que estamos hablando de un nivel de madurez L4 gestionado y medible.

Al tratarse del mismo activo, el riesgo va degradándose por cada control implementado. En el caso del ejemplo, se tiene un riesgo residual de 9= medio por tener implementada la medida «control de acceso», por lo que a ese riesgo medio hay que restar los valores del segundo control implementado. En este caso, el procedimiento de control de accesos lógico; posteriormente, el control de autenticación de doble factor; luego la seudonimización; y finalmente el almacenamiento del archivo, testando datos personales en la base ya disociada.

Control(es) implementado(os)	*Reduce Probabilidad*	*Reduce impacto*				*Riesgo residual*	*Madurez de la medida*
		C	*I*	*D*	*IT*		
Control de accesos-usuario y contraseña	Sí; reduce de 4a a 3- media	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	9= Medio	L2
Política de control de accesos lógico	Sí; pasa de 3 a 2-baja	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	6= Medio	L4
Control de accesos-autenticación doble factor	Sí; reduce de 2 a 1-muy baja	No; queda en 3	No; queda en 3	No; queda en 2	3-Medio	3= Bajo	L4
Seudonimización	No; hereda el nivel 1 de la medida anterior	Sí; reduce de 3 a 2	Sí; reduce de 3 a 2	No; queda en 2	2-Bajo	2= Muy bajo	L4
Digitalizado en versión pública sin vincular al titular	No; hereda el nivel 1 de la medida anterior	Sí; reduce de 2 a 1	Sí; reduce de 2 a 1	Sí; reduce a 1	1-Muy bajo	1= Muy bajo	L4

Tabla 20. Elaboración propia.

Con estas cuatro medidas de seguridad, el riesgo residual resulta en Muy bajo, por lo que no tendría que tratarse, pero sí monitorearse. Así debe quedar planteado en el plan de trabajo y en el plan de monitoreo y revisión. Esto además de la mejora de los niveles de madurez de las medidas ya implementadas, como se verá en el siguiente título.

ETAPA 5

PLAN DE TRABAJO

Una vez realizado el análisis de riesgos y el de brecha, debe priorizarse en la atención o tratamiento a los riesgos de mayor nivel, de los activos más críticos. De las medidas seleccionadas en el análisis de brecha, deberán establecerse los plazos, los pasos a seguir y las personas responsables de implementarlas, es decir, debe definirse un plan de trabajo.

Para ello, es necesario utilizar los resultados de los análisis mencionados, a fin de que sean la base para la planeación de las actividades a realizar con miras a tratar los riesgos que se han identificado en los sistemas de tratamiento y los datos personales, según el análisis de brecha.

El plan de trabajo puede equipararse a lo que en materia de gestión del riesgo es el plan de tratamiento del riesgo o plan director, el cual debe definir las acciones a implementar para tratar el riesgo, establecer las prioridades de atención de riesgos específicos y su período. Dicha prioridad puede establecerse equilibrando la valoración del riesgo y el análisis costo-beneficio de la implementación en relación con el presupuesto.

Por ello, en atención a la *Ley General* y *Lineamientos Generales*, los sujetos obligados deberán atender 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. [...]

IV. [...]

V. [...]

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*:

«Plan de trabajo

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.»

El plan de trabajo es parte medular del *Documento de seguridad*. En éste deben detallarse las acciones tomadas para implementar las medidas de seguridad. Para ello se deberá priorizar el tratamiento de los riesgos más urgentes (Muy alto y Alto), seleccionando las medidas de seguridad idóneas que reduzcan el riesgo actual en la entidad. Esto es, que se elijan las medidas de seguridad según el contexto del sujeto obligado. Además, se deben especificar los recursos del tipo económico, humano o de cualquier naturaleza que se requieren para su implementación. Se deberá indicar si existe presupuesto para implementar o fortalecer las medidas, quiénes serán las personas servidoras públicas responsables de implementarla y en qué período, pudiéndose desglosar incluso por etapas.

ETAPA 6

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

En esta etapa, se deben evaluar y medir los resultados de la implementación de las medidas de seguridad. Es decir, se debe verificar que las medidas realmente se estén aplicando dentro del sujeto obligado y que éstas funcionen para la correcta gestión del riesgo. Para ello es indispensable monitorear con debida anterioridad si existen nuevos tratamientos de datos personales, nuevas amenazas, vulnerabilidades, y si las medidas de seguridad son acordes y suficientes para el nivel de riesgo asociado.

Al respecto, la *Ley General* y los *Lineamientos Generales* consignan:

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. [...]

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

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 implementada, 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.»

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. 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;»

Artículo 63 de los *Lineamientos Generales*:

«Monitoreo y supervisión periódica de las medidas de seguridad implementadas

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.»

Artículo 35 de la *Ley General*:

«De manera particular, el responsable deberá elaborar un *Documento de seguridad* que contenga, al menos, lo siguiente:

I. [...]

II.

III.

IV.

V. Los mecanismos de monitoreo y revisión de las medidas de seguridad [...]»

La *Ley General*, por medio del principio de responsabilidad, establece que debe implementarse un sistema de supervisión y vigilancia para la comprobación del cumplimiento de las políticas internas de seguridad. Dicha obligación debe observarse en armonía con los demás artículos que refieren a los mecanismos de monitorización de las medidas de seguridad, incluyendo las políticas internas, en tanto que éstas son medidas de seguridad administrativas.

Por su parte, el artículo 49 de los *Lineamientos Generales* consigna que el responsable deberá revisar las políticas y programas de seguridad al menos cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, se requiera una actualización previa. En ese contexto, se busca que las medidas de seguridad estén en constante revisión, evaluación y actualización: es decir, es un ciclo de mejora continua.

El artículo 33 de la *Ley General* que establece los mínimos requeridos para el establecimiento de medidas de seguridad de los datos personales dentro del sujeto obligado prescribe que se debe monitorear y revisar de modo periódico las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales. Esto es así porque, para valorar si las medidas de seguridad realmente están funcionando, deben analizarse o monitorearse previa y regularmente los niveles de riesgo a los que están expuestos los datos personales. Esto es, revisar las nuevas amenazas que puedan explotar sus vulnerabilidades, nuevas vulnerabilidades y los factores de riesgo, para posteriormente evaluar si las medidas de seguridad están operando y, de ser así, si realmente están mitigando los factores del riesgo.

Lo anterior se reitera en el artículo 63 de los *Lineamientos Generales*, al establecer que el responsable debe 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 si se están cumpliendo los objetivos de seguridad planteados, y para ello es necesario monitorear los nuevos activos (datos personales y sistemas del tratamiento), modificaciones en el modo de tratar los datos, como la implementación de sistemas automatizados o nuevas tecnologías para el tratamiento de datos personales, las nuevas amenazas, nuevas vulnerabilidades de los activos, viejas vulnerabilidades que puedan reaparecer y no se hayan valorado recientemente, cambios en los factores del riesgo, esto es en el impacto que pueden causar las amenazas en los activos y en las personas titulares de los datos personales o cambios en la probabilidad de ocurrencia de vulneraciones, que resulten en un cambio del nivel del riesgo a uno mayor e inaceptable.

Asimismo, el último párrafo del artículo 63 establece que 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. Debe considerarse que la monitorización y revisión del sistema de gestión no sólo involucra la monitorización y revisión de las medidas de seguridad, sino también toda la planeación e implementación del propio sistema. En ese sentido, se deberá establecer un programa de auditorías en particular para el SGSDP, siendo posible que los resultados de dichas auditorías incidan en la actualización de medidas de seguridad, o bien en modificaciones a todo el sistema, lo que repercutirá en el *Documento de seguridad*.

La actualización y mejora continua de las medidas de seguridad (y por tanto del sistema de gestión y el *Documento de seguridad*) es la consecuencia lógica del trabajo de monitoreo, revisión y evaluación de las medidas de seguridad y del propio SGSDP. Al respecto, la *Ley General* y los *Lineamientos Generales* establecen los supuestos específicos donde deben actualizarse las medidas de seguridad que se detallarán adelante. Sin embargo, es importante aclarar que no es necesario esperar a dichos momentos para hacerlo: de implementarse bien un sistema de gestión, y que se monitoreen debidamente los activos, sus vulnerabilidades, amenazas y el riesgo en general, es probable que las medidas de seguridad deban actualizarse incluso antes de materializarse los supuestos a que refiere la normativa en la materia.

Respecto a los supuestos de actualización establecidos en la Ley, en primera instancia se encuentra el artículo 30, fracciones IV y V de la *Ley General*, que establece que 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 congruencia con esto, el artículo 36 de la *Ley General* refiere específicamente los momentos en que el responsable debe actualizar el *Documento de seguridad*, y que son en particular, cuando:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales, que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; o
- Cuando se implementen acciones correctivas y preventivas ante una vulneración de seguridad.

De la observación de estos supuestos, puede concluirse que las actualizaciones son consecuencia de lo realizado en la monitorización y revisión tanto de los activos y la valoración del riesgo como de la revisión de las medidas de seguridad. Por ello deben contemplarse estos supuestos para la implementación de los mecanismos de monitoreo y revisión.

Los mecanismos de monitoreo deben cumplir con todos los requerimientos que exigen los numerales citados con antelación. Estos mecanismos deben estar armonizados para todas las medidas de seguridad, incluyendo las políticas y programas de seguridad y tratamiento de datos personales. Asimismo debe tenerse claro que, de cambiar alguna medida por actualización o mejora, esto debe verse reflejado tanto en el sistema de gestión como en el *Documento de seguridad*.

Para cumplir con los mecanismos de monitoreo y revisión, será necesario determinar cómo se van a monitorear, medir, analizar y actualizar las medidas de seguridad, a través de la propia implementación de una política que describa el proceso a seguir para dicho monitoreo, análisis, evaluación y actualización.

Revisión de los Factores de riesgo

Se debe monitorear y revisar el riesgo con sus factores relacionados. Es decir, el valor de los activos, las amenazas, las 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.

Las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin aviso alguno. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas. Por ello se requiere de constante monitoreo para detectar esos cambios. Por ejemplo, es posible apoyarse en servicios externos que provean información respecto a las amenazas o vulnerabilidades.

Los sujetos obligados deben asegurar que los siguientes puntos estén continuamente monitoreados:

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

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

El resultado del monitoreo de riesgo puede afectar su tratamiento y aceptación, y en consecuencia el contexto que se establezca en un ciclo de mejora continua.

Sistema de monitoreo

El objetivo de este tipo de sistemas es la alerta temprana frente a la concreción de incidentes de seguridad de la información y la recolección de métricas que son fundamentales para la gestión de seguridad de la información.

Las métricas provenientes del monitoreo deberán complementar la evaluación de los procesos y políticas de seguridad, brindando información relevante para realizar la gestión de riesgos, lo que a la vez permita argumentar frente al Comité de Transparencia o responsable del tratamiento qué políticas o controles deben reformularse o reforzarse.

Para implementar cualquier tipo de sistemas de monitoreo, puede incluso utilizar herramientas o *software* especializado. Lo que debe buscar es encontrar una herramienta que le permita:

- Implementar y operar un sistema de mediciones de seguridad.
- Recolectar y analizar datos.
- Mostrar gráficamente los resultados de las mediciones.
- Comunicar los resultados de las mediciones desarrolladas a las principales partes interesadas.
- Utilizar los resultados de las mediciones como apoyo a la toma de decisiones relacionadas con la seguridad.
- Utilizar los resultados de las mediciones para identificar necesidades de mejora.

Si se determina que se puede utilizar un *software* de monitoreo, debe considerarse los siguientes elementos centrales:

1. La instalación y configuración de programas de monitoreo de plataforma;
2. La implementación de un *software* para administración de registro de incidentes reportados por los usuarios;
3. La definición del conjunto de reportes que contendrían las métricas para informar a los niveles directivos el estado de salud de la seguridad de la información.

Auditoría

Como establece el último párrafo del artículo 63 de los *Lineamientos Generales*, se debe contar con un programa de auditoría interna y/o externa para monitorear y revisar la eficacia y eficiencia del SGSDP. Este programa debe planearse, establecerse y mantenerse considerando la política de gestión de datos personales. En su caso, deben considerarse auditorías a través de externos, para procesos y circunstancias especiales. Por ejemplo, cuando el sujeto obligado desea unirse a un esquema de certificación.

Deben establecerse con considerable anterioridad los objetivos del programa de auditoría. Éste 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.

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

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

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

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

La auditoría debe ofrecer al responsable información detallada respecto a cambios ocurridos en el SGSDP. Además, debe realizarse una auditoría inmediatamente después de la implementación de modificaciones mayores en el SGSDP o en los procesos críticos del sujeto obligado respecto al tratamiento de datos personales.

Como resultado de una auditoría, deben obtenerse observaciones sobre riesgos existentes para aplicar medidas preventivas. Es decir, controles para que no ocurra una vulneración,

así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

Aunado a lo anterior, se debe recordar que los sujetos obligados podrán someterse a auditorías voluntarias 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.

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.»

Vulneraciones a la Seguridad de la Información

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.»

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

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

1. Identificación de la vulneración. En caso de un incidente de seguridad, la organización debe identificar:
   a. Los activos afectados junto con el personal a cargo;
   b. Los titulares afectados;
   c. Las partes interesadas que requieran estar informadas y/o puedan tomar parte en la toma de decisiones para mitigar las consecuencias de la vulneración.
2. Notificación de la vulneración. Una vez identificada la vulneración, ésta debe comunicarse a los titulares de los datos personales, para que puedan tomar medidas que mitiguen o eviten una posible afectación.

Artículo 66 de los *Lineamientos Generales*:

«Plazo para notificar las vulneraciones de seguridad

De conformidad con lo dispuesto en el artículo 40 de la *Ley General*, el responsable deberá notificar al titular y al Instituto las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro en un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

El plazo a que se refiere el párrafo anterior comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

Para efectos del presente artículo, se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de modo enunciativo mas no limitativo, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

Para los efectos del presente artículo, se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de modo enunciativo mas no limitativo, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.»

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

Artículo 40 de la *Ley General*:

«El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.»

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

Artículo 41 de la *Ley General*:

«El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata; y

V. Los medios donde puede obtener más información al respecto.»

Artículo 67 de los *Lineamientos Generales*:

«Notificación de las vulneraciones de seguridad al Instituto

En la notificación a que se refiere el artículo anterior, el responsable deberá informar mediante escrito presentado en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:

I. La hora y fecha de la identificación de la vulneración;

II. La hora y fecha del inicio de la investigación sobre la vulneración;

III. La naturaleza del incidente o vulneración ocurrida;

IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;

V. Las categorías y número aproximado de titulares afectados;

VI. Los sistemas de tratamiento y datos personales comprometidos;

VII. Las acciones correctivas realizadas de forma inmediata;

VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;

IX. Las recomendaciones dirigidas al titular;

X. El medio puesto a disposición del titular para que pueda obtener más información al respecto;

XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse; y

XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.»

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

Artículo 37 de la *Ley General*:

«En caso de que ocurra una vulneración a la seguridad, el responsable deberá 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.»

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad deben estar debidamente documentados, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas, con el fin de que el sujeto obligado cuente con evidencia suficiente para mostrar al Instituto su diligencia en tomar las acciones necesarias que eviten o mitiguen una vulneración a la seguridad de los datos personales.

Mejora Continua

El monitoreo de los factores de riesgo y los resultados de las auditorías proporcionan información para demostrar la eficacia de la seguridad de la información, específicamente del Sistema de Gestión de Seguridad de Datos Personales; y también presentan las áreas de oportunidad donde éste puede ser mejorado.

Los puntos de mejora pueden corresponder a dos tipos:

a. **Acciones correctivas:** Encaminadas a eliminar las causas de fallas o incidentes ocurridos en el SGSDP, para prevenir que vuelvan a ocurrir. Dichas acciones deben ser proporcionales a la gravedad del incidente. Las acciones correctivas deben atenderse considerando:

- El análisis y revisión de la falla o incidente;
- Determinar las causas que dieron origen a la falla o incidente;

- Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
- Determinar e implementar las acciones necesarias;
- Registrar los resultados de las acciones tomadas;
- Revisar la eficacia de las acciones correctivas tomadas.

b. **Acciones preventivas:** Encaminadas a eliminar las causas de fallas o incidentes posibles. Dichas acciones deben ser proporcionales a las amenazas potenciales. Las acciones preventivas deben atenderse considerando:

- El análisis y revisión de la amenaza;
- Determinar las fallas o incidentes que podrían desencadenarse con una amenaza;
- Evaluar las acciones necesarias para evitar que la falla o incidente ocurra;
- Determinar e implementar las acciones necesarias;
- Registrar los resultados de las acciones tomadas;
- Revisar la eficacia de las acciones preventivas tomadas.

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

En función de las acciones correctivas y preventivas, así como de la actualización del contexto del sujeto obligado resultado del monitoreo del riesgo, deben establecerse o mejorarse los planes de capacitación.

ETAPA 7

PROGRAMA GENERAL DE CAPACITACIÓN

En esta etapa, el sujeto obligado deberá generar un programa que especifique el tipo de capacitación que requieren sus servidores públicos, definido a partir de las actividades que realizan las personas que intervienen en el tratamiento de datos personales que se ha identificado desde la elaboración del inventario de datos personales o sistemas de tratamiento y en el apartado de funciones y obligaciones de las personas que tratan datos personales.

Conforme a la *Ley General* y a los *Lineamientos Generales*, el sujeto obligado deberá atender lo siguiente:

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; […]»

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:
[...]

I. 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 éstos;

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, según 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 diversos niveles de capacitación del personal bajo su mando, dependiendo de los roles y responsabilidades que les corresponden en el tratamiento de los datos personales.

En el programa general de capacitación se debe contemplar una a nivel general en materia de datos personales, pero también en materias específicas según los roles y responsabilidades de los servidores públicos en el tratamiento de datos personales que realizan en particular.

Debe comprenderse que la mejor medida de seguridad contra posibles vulneraciones es contar con personal capacitado y consciente de sus responsabilidades y deberes respecto a la protección de datos personales. Si bien, todos requieren una capacitación general en materia de protección de datos personales respecto a los contenidos y conceptos de la *Ley General*, sus principios, deberes y obligaciones, algunos requerirán un distinto nivel de capacitación técnica, 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 una capacitación más técnica y especializada que aquél cuya función sea recabar datos personales en un formato físico y que no contenga datos personales sensibles. 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.

El programa de capacitación debe contemplar, además de la capacitación a distintos niveles de especialización de acuerdo con los roles y responsabilidades que desempeñan los servidores públicos, objetivos de capacitación respecto a la temporalidad:

a. Concienciación: Programas a corto plazo para la difusión en general de la protección de datos personales en el sujeto obligado;
b. Entrenamiento: Programas a mediano plazo que tienen por objetivo capacitar al personal de modo específico respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales; y
c. Educación: Programa general a largo plazo cuyo objetivo es incluir la seguridad en el tratamiento de los datos personales dentro de la cultura del sujeto obligado.

Por ello debe realizarse una detección de necesidades, para identificar el nivel y tipo de capacitación necesaria para el personal, según las responsabilidades asignadas y considerando su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Estos programas de capacitación deben priorizar elementos como:

a. Requerimientos y actualizaciones al contexto del SGSDP, considerando principalmente:

   1. la administración y comunicación de noticias de privacidad;
   2. el manejo de solicitudes y quejas de los titulares;
   3. la recolección y manipulación de datos personales;
   4. la gestión de incidentes y vulneraciones de seguridad; y
   5. la gestión de seguridad con terceros.

b. La legislación en protección de datos personales y 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.

Se recomienda evaluar la eficiencia y eficacia de la capacitación. Esta evaluación puede verificarse 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. Deben establecerse 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.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El *Documento de seguridad*, como aquél donde se plasman contenidos que deben ir de la mano del SGSDP, debe comprenderse como un documento vivo que está sujeto a modificaciones recurrentes, en tanto que se busca la mejora continua en materia de seguridad de los datos personales. Por ello, una vez elaborado, deberá conocerse que hay supuestos por los cuales dicho documento debe ser actualizado conforme a la *Ley General*. Por ejemplo:

- Por presentar modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de mejora continua;
- Como resultado de un proceso derivado de una vulneración de seguridad;
- Como parte de acciones correctivas o preventivas ante una vulneración.

Específicamente en la *Ley General* se menciona:

Artículo 36 de la *Ley General*:

«El responsable deberá actualizar el *Documento de seguridad* cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; e

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.»

ANEXO A
FORMATO DE INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

CABECERA DEL DOCUMENTO

Unidad administrativa	Asentar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización	Consignar fecha en que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso)	Especificar nombre del tratamiento.
Fundamento jurídico que habilita el tratamiento	Detallar las principales disposiciones normativas, artículos, apartados, fracciones, incisos, párrafos de los que deriva el tratamiento en cuestión.
Atribuciones de la unidad administrativa para realizar el tratamiento	Incluir las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento; entre ellas, las que señala el Reglamento o Estatuto Orgánico interno, y otras si las hubiere.

PARTE 1 – MEDIOS DE OBTENCIÓN

Medio de obtención de los datos personales (1)			*Tercero que transfiere los datos personales, en su caso* (2)	*Finalidades de la transferencia recibida, en su caso* (3)
Informar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, deberá indicarse un medio por fila.	Describir el medio; por ejemplo, la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción Otro, especificar el medio de obtención.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, consignar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se asentó que los datos personales se reciben por transferencia, consignar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere los datos personales.

PARTE 2 – TIPOS DE DATOS

Listado de datos personales (4)	*Sensible (5)*	
Señalar cada uno de los datos personales que se tratan, o sus categorías, uno por fila.	En caso de seleccionar la opción Otro, especificar.	Asentar si el dato personal es sensible o no.

PARTE 3 – FORMATO Y UBICACIÓN DE LOS DATOS

Formato de la base de datos (6)	*Ubicación base de datos (7)*		*Sección de archivos (8)*	*Serie de archivos (9)*	*Subserie de archivos (10)*
Consignar el o los formatos en los que se encuentra la base de datos del tratamiento.	Informar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.	Indicar clave de identificación de la sección a la que corresponde el tratamiento.	Asentar clave de identificación de la serie a la que corresponde el tratamiento.	Detallar clave de identificación de la subserie a la que corresponde el tratamiento.

PARTE 4 – FINALIDADES DE TRATAMIENTO

Finalidades del tratamiento (11)	*¿Requiere consentimiento? (12)*	*Supuesto artículo 22 que se actualiza, en su caso (13)*	*Tipo de consentimiento (14)*
Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.	Asentar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, indicar el o los supuestos del artículo 22 de la LGPDPPSO que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, detallar el tipo de consentimiento que se necesita.

PARTE 5 – SERVIDORES PÚBLICOS CON ACCESO A LOS DATOS

Servidores públicos que tienen acceso a la base de datos (15)	*Área de adscripción (16)*	*Finalidad del acceso (17)*
Asentar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	Definir unidad administrativa a la que está adscrito el puesto.	Especificar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.

PARTE 6 - ENCARGADO

Nombre del encargado, en su caso (18)	*N.° de contrato, pedido o convenio con el encargado, o del instrumento jurídico correspondiente (19)*
Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Incluir el número de identificación del instrumento jurídico que regula la relación con el encargado.

PARTE 7 – TRANSFERENCIAS DE DATOS

¿Se realizan transferencias? (20)	*Tercero al que se transfieren los datos personales, en su caso (21)*	*Finalidades de la transferencia (22)*	*¿Requiere consentimiento la transferencia? (23)*	*Supuestos artículos 22, 66 ó 70 que se actualizan, en su caso (24)*	*Tipo de consentimiento que se requiere para la transferencia (25)*	*¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (26)*	*Supuesto artículo 66 que se actualiza, en su caso (27)*
Indicar si se realizan o no transferencias en el marco del tratamiento.	Asentar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien su categoría. Uno por fila.	Detallar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Indicar si la transferencia requiere o no consentimiento.	En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	En caso de que la finalidad de la transferencia requiera el consentimiento del titular, consignar si se requiere el tácito o el expreso y por escrito.	Asentar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO.	Informar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.

PARTE 8 – DIFUSIÓN DE LOS DATOS

Difusión de los datos personales (28)	*Fundamento jurídico para la difusión (29)*
Precisar si en el tratamiento se realiza la difusión de los datos personales.	Asentar el fundamento jurídico que ordena la difusión de los datos personales.

PARTE 9 – PLAZO DE CONSERVACIÓN Y BLOQUEO

Plazo de conservación (30)	*Bloqueo (31)*	*Observaciones*
Informar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística.	Detallar período en el que estarán bloqueados los datos personales.	Espacio libre para hacer aclaraciones y precisiones.

La *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* establece que cada responsable deberá elaborar un *Documento de seguridad*. Al tiempo lo define como un instrumento que describe y da cuenta, de modo general, sobre las medidas de seguridad, técnicas, físicas y administrativas que adopte para garantizar confidencialidad, integridad y disponibilidad de los datos personales que posee.

En ese orden, de conformidad con el artículo 35 de la *Ley General*, dicho documento debe contener al menos el inventario de datos personales y de los sistemas de tratamiento, funciones y obligaciones de quienes tratan datos personales, el análisis de riesgos, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación.

INAImx inai_mx INAImexico

inaimexico inai.org.mx 800 835 43 24

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