RECOMENDACIONES PARA RECONOCER LAS PRINCIPALES AMENAZAS A LOS DATOS PERSONALES

A PARTIR DE LA **VALORACIÓN RESPECTO AL RIESGO**

inai

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidente

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

Rosendoevgeni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

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

Edición Abril 2021.

CONTENIDO

PRESENTACIÓN

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

La valoración del riesgo identifica los activos existentes, las **amenazas** aplicables, y los escenarios de vulneración.

De esta manera, a partir de la identificación de circunstancias o eventos con la capacidad de causar daños a la organización (amenazas) como parte del ánalisis de escenarios en los que las amenazas explotan la falta o debilidad de seguridad en un activo, se pretende ayudar a los Responsables y Encargados del tratamiento de datos personales a identificar y catalogar las principales amenazas, como parte de la gestión de riesgos, a las que se pueden enfrentar los datos personales que resguardan.

IR AL CONTENIDO

OBJETIVO

Conformar un documento de apoyo para los Responsables (tanto de sector público como del sector privado) con el que puedan identificar las principales amenazas a los datos personales contenidos en los diversos sistemas de tratamiento, así como obtener elementos que les permitan describir categorizar y ponderar el riesgo respecto de dichas amenazas.

Una vez identificadas las amenazas a las que están expuestos los diversos sistemas de tratamiento, los responsables podrán realizar una identificación de las vulnerabilidades en sus sistemas e implementar las medidas de seguridad necesarias (físicas, técnicas o administrativas) o bien adecuar las existentes y con ello reducir la posibilidad de un daño a sus sistemas de tratamiento.

IR AL CONTENIDO

DEFINICIONES

Activo: Todo elemento de valor para una organización, involucrado en el tratamiento de datos personales,[1] entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

Encargado: la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.[2]

La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.[3]

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

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

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

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

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

1 En el Anexo A, de la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf, podrá consultar ejemplos de activos.

2 Definición de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

3 Definición de la Ley General de Protección de Datos Personales en Posesión de los Particulares

IR AL CONTENIDO

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

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

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

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

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

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

Tratamiento: 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.[4]

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.[5]

4 Definición de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

5 Definición de la Ley General de Protección de Datos Personales en Posesión de los Particulares

IR AL CONTENIDO

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

Identificar el riesgo: Proceso para encontrar, enlistar y describir los elementos del riesgo. Valorar el riesgo. Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

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

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

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

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

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

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

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

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

IR AL CONTENIDO

REFERENCIAS NORMATIVAS

SECTOR PÚBLICO

Artículo 33, fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[6] (LGPDPPSO), señala:

> Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:
>
> (…)
> IV. Realizar un análisis de riesgo de los datos personales, considerando las **amenazas** y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
>
> VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
> (…)

Artículo 63, fracciones III, IV, V y VI, de los Lineamientos Generales para la Protección de Datos Personales en el Sector Público[7] (Lineamientos Generales), que indica:

> Monitoreo y supervisión periódica de las medidas de seguridad implementadas
>
> Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y

6 Publicada en el Diario Oficial de la Federación el 26 de enero de 2017, https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

7 Publicados en el Diario Oficial de la Federación el 26 de enero de 2018, https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

IR AL CONTENIDO

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:

(…)

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

(…)

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.

SECTOR PRIVADO

En la misma línea de ideas, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,[8] señala en su artículo 61, fracción III lo siguiente:

III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;

8 Reglamento de la LFPDPPP, publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011, http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

IR AL CONTENIDO

Por su parte las Recomendaciones en materia de seguridad de datos personales,[9] en su numeral 2.1, denominado conceptos clave, se indica:

> **Incidente.** Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.
>
> **Amenaza.** Circunstancia o evento con la capacidad de causar daño a una organización.
>
> **Vulnerabilidad.** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más **amenazas**.
>
> **Riesgo de seguridad.** Potencial de que cierta **amenaza** pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

9 Publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013, https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

IR AL CONTENIDO

INTRODUCCIÓN

Antes de iniciar es necesario abordar una serie de conceptos base interrelacionados en la gestión de riesgos, los cuales son: activo, amenaza, vulnerabilidad, impacto y probabilidad.

Como se señaló en las definiciones, un activo es todo elemento de valor para una organización o responsable, involucrado en el tratamiento de datos personales, por ejemplo: la base de datos de empleados, el registro de acceso a un edificio, los equipos de cómputo de una oficina, el correo electrónico o el almacenamiento de información en la nube.

Estos activos son susceptibles a **amenazas**, es decir, a factores externos que tienen el potencial de dañarlos, podemos mencionar algunos como: una descarga eléctrica que puede dañar un equipo de cómputo, o un empleado quién podría acceder a información sin que esté autorizado para ello.

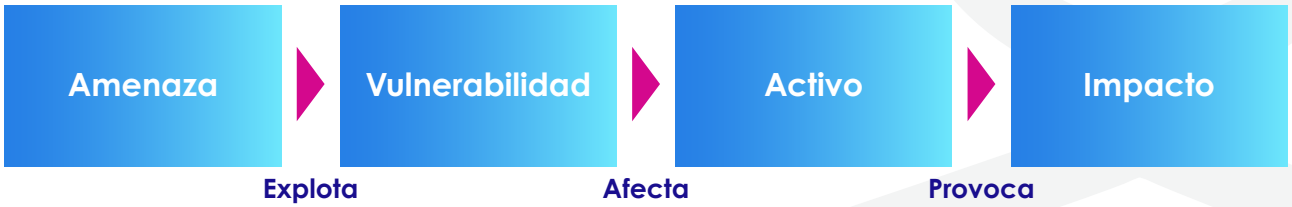
Para que una amenaza tenga efecto, requiere explotar una **vulnerabilidad**, debilidad o falla propia de un activo, así tenemos que, la descarga eléctrica sólo puede afectar a los equipos de cómputo que no tengan un regulador de voltaje. Por otro lado, el empleado podría acceder sin autorización a una base de datos si, esta, no está protegida con contraseña.

IR AL CONTENIDO

Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos:

RIESGO

Existe una **posibilidad** de ocurrencia de que un riesgo se materialice; cuando esto sucede, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.



GESTIÓN DE RIESGOS

Las actividades llevadas a cabo para mantener el riesgo por debajo de un umbral fijado se denominan Gestión del riesgo. Para gestionar el riesgo, deberá realizar lo siguiente:

1. **Analizar el riesgo,** es decir, averiguar el nivel de riesgo que se está soportando.

2. **Tratar el riesgo,** para aquellos riesgos cuyo nivel está por encima del umbral deseado se debe decidir cuál es el mejor tratamiento que permita disminuirlos.

Por lo que la Gestión de riesgos es **=** Análisis de riesgos **+** Tratamiento de riesgos.

IR AL CONTENIDO

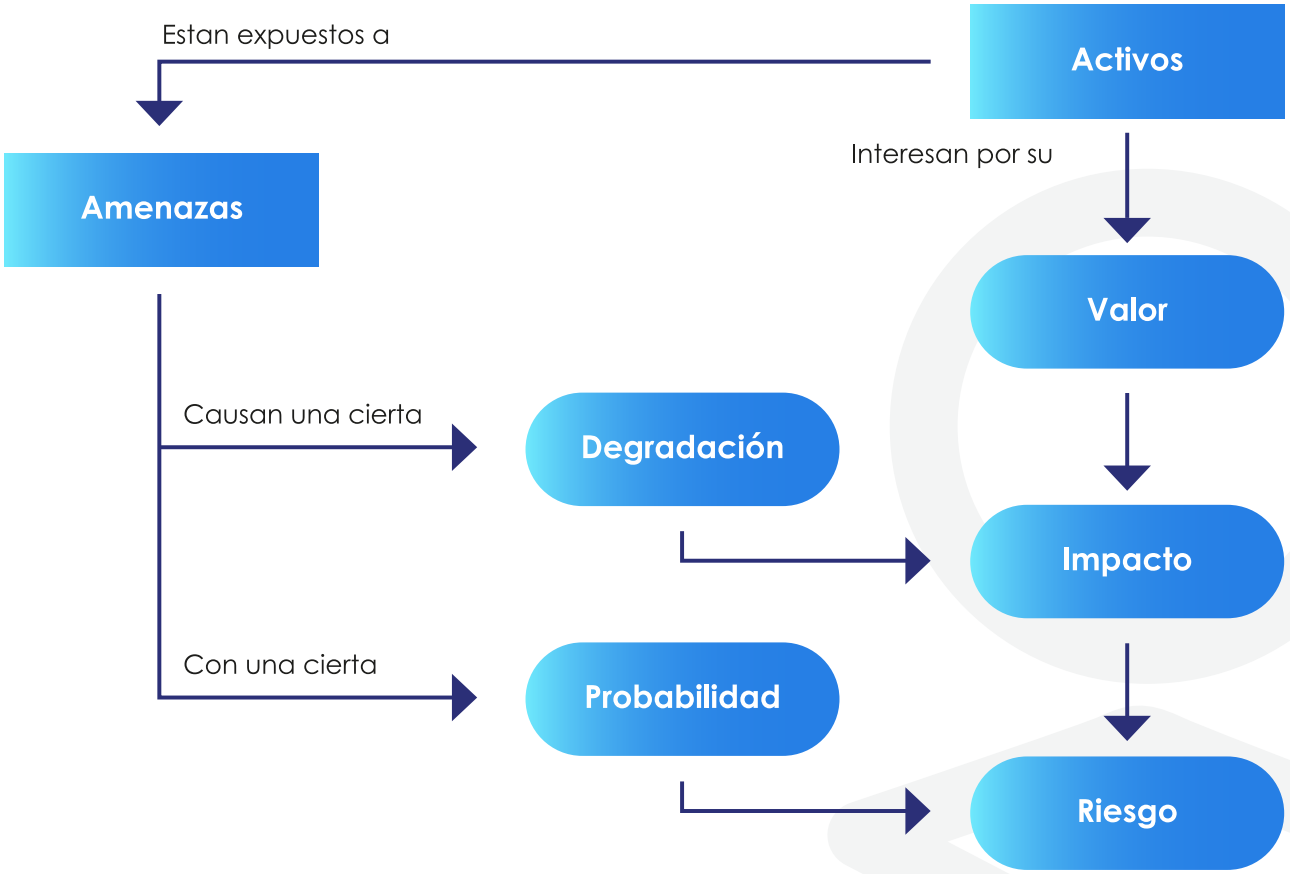
VALORACIÓN RESPECTO AL RIESGO

La valoración del riesgo identifica los activos existentes, las amenazas aplicables, y los escenarios de vulneración.

Partiendo de la valoración del riesgo, podemos mencionar lo siguiente:

- Primero es importante identificar los activos que se van a proteger, ya que, a partir de estos, se van a identificar los vulnerabilidades y amenazas a los que se enfrentan dichos activos.
- Entre las vulnerabilidades y las amenazas, existe una estrecha relación, ya que sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.
- Para que una amenaza represente un riesgo, se requiere de que el activo tenga un interés por su valor, y que la amenaza, al ser explotada, cause cierta degradación a la seguridad; lo que podría impactar a los activos.
- El nivel de riesgo es una estimación de lo que puede ocurrir, y se valora de forma cuantitativa como el producto del impacto (consecuencia) –asociado a una amenaza (suceso)– por la probabilidad de la misma.

IR AL CONTENIDO



Elementos del análisis de riesgos potenciales[10]

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

- Daños personales
- Pérdidas financieras
- Interrupción de servicios
- Pérdida de reputación

10 Para su consulta: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

IR AL CONTENIDO

La valoración de los riesgos es una aproximación metódica para determinar el riesgo, siguiendo los siguientes pasos:

01 Identificar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación.

02 Identificar las amenazas a las que estan expuestos los activos identificados.

03 Valorar las amenazas.

04 Estimar el daño sobre el activo, derivado de la materialización de la amenaza identificada, es decir, el impacto.

05 Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

PASO 1. IDENTIFICAR ACTIVOS

Un activo puede ser un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Para este documento, los activos que tienen valor y requieren resguardarse son los datos personales, recordando que estos activos conviven con otros activos como lo son: servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

IR AL CONTENIDO

De esta manera, se pueden identificar dos tipos de activos:

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

Es importante que mantenga actualizado su inventario de activos, así como los medios de almacenamiento en que residen las bases de datos personales.

Después de identificar y describir los activos de información y de apoyo, se podrán encontrar sus vulnerabilidades y posibles amenazas.

PASO 2. IDENTIFICAR AMENAZAS

Cuando hablamos de seguridad de la información hablamos de protegerla de riesgos que puedan afectar a una o varias de sus tres principales propiedades:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
• Acceso ilegítimo a los datos • *¿Qué daño causaría que lo conociera quien no debe?*	• Modificación no autorizada de los datos • *¿Qué perjuicio causaría que el dato estuviera dañado o se presume como corrupto?*	• Eliminación de los datos • *¿Qué perjuicio causaría no tener un dato o no poder utilizarlo?*

IR AL CONTENIDO

Las amenazas son "acciones que ocurren" y que pueden causarle daño a nuestros activos, son muy variadas y van cambiando con el tiempo.

Es importante mencionar que, no todas las amenazas afectan a todos los activos, sino que hay cierta relación entre el tipo de activo y lo que le podría ocurrir.
Las amenazas se dividen en grupos como:

1. **Del entorno (de origen industrial).**
   Se obtienen del análisis del entorno que rodea la organización y pueden dividirse en dos tipos:
   a) **Internas.** Aquellas que tienen como origen un elemento dentro de la organización o responsable.
   b) **Externas.** Aquellas que tienen como origen un elemento fuera de la organización o responsable.

2. **De origen natural.**
   Son aquellas que tienen como origen un acto que no es atribuible a acciones u omisiones de una persona, estas son amenazas causadas por fenómenos naturales, que pueden agruparse en:
   a) **Sismicidad,** vibración del suelo, amplificación espectral, aceleración de intensidad, ruptura del suelo; que pueden derivar en: ruptura del suelo, licuefacción, tsunami, deslizamiento, levantamiento y hundimiento cortical.
   b) **Volcanismo,** erupciones, flujos de piroclastos, tsunami, coladas de lava, emisión de gases, vapores, lluvia acida.
   c) **Hidrometeorología,** ciclones, granizadas, precipitaciones, heladas, frentes polares, tornados, convergencia intertropical, vaguadas, que pueden derivar en lluvias intensas, sequías o vientos.
   d) **Deslizamiento de tierra,** destrucción de laderas, aludes, avalanchas, represamiento de cauces fluviales.
   e) **Erosión,** remoción de suelos y nutrientes, destrucción de laderas, sovocación, sedimentación de riveras.
   f) **Avalanchas,** escorrentía torrencial, destrucción de laderas, lechos fluviales, causes.
   g) **Tormentas eléctricas,** nubes cumulonimbus que producen truenos, rayos, lluvias fuertes, vientos en ráfagas, y pueden incluso formar granizo y tornados.

IR AL CONTENIDO

3. **De origen tecnológico**.
   Amenazas causadas por la actividad industrial, las tecnologías, maquinarias y construcciones creadas por el hombre.
   a) **Dispositivos electrónicos y sistemas,** bajo esta denominación podemos contemplar todas las vulnerabilidades de los equipos informáticos, software y hardware.
   b) **Red,** cada día es menos común que una máquina trabaje aislada, por lo que en esta categoría se deben incluir todos los elementos que son necesarios para una interconexión o comunicación entre dispositivos.

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas, es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad,

4. **De origen humano.**
   Aquellas que tienen como origen un acto atribuible a una persona. Estas a su vez pueden ser clasificadas en:
   a) **Accidentales.** Aquellas en las que no existió una voluntad para generarla; las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
   b) **Deliberadas.** Aquellas en las que existe voluntad de generarlas. Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Es importante que por cada amenaza identificada registre la siguiente información:

- Antecedentes.
- Explicación del efecto de la amenaza.

Como resultado de este paso, debe identificar las amenazas significativas sobre los activos identificados, tomando en consideración el tipo de activo y la dimensión sobre el valor del activo.

PASO 3. VALORAR LAS AMENAZAS

Cuando un activo es víctima de una amenaza, no se ve afectado en su totalidad, una vez que se ha identificado la amenaza que puede perjudicar al activo, se debe valorar la influencia en el valor del activo en dos sentidos:

- **Degradación:** que tan perjudicado resultaria el valor del activo.
- **Probabilidad:** cuan probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera y suele representarse con una valoración:

Muy alta
Alta
Media
Baja
Muy baja

En cuanto a la probabilidad de ocurrencia, esta es más compleja de determinar y expresar; a veces se modela de manera cualitativa por alguna escala nominal, otras se modelan numéricamente o como frecuencia de ocurrencia:

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Anualmente
1/10	Poco frecuente	Cada determinados años
1/100	Muy poco frecuente	Por siglos

En este paso se valoran las amenazas identificadas en la tarea anterior, tomando en consideración elementos como la experiencia.

IR AL CONTENIDO

Es importante que por cada amenaza identificada registre la siguiente información:

- Estimación de la frecuencia.
- Estimación del daño que causaría su materialización.

Una recomendación para la evaluación de la probabilidad de ocurrencia de la amenaza, es tomar en cuenta los siguientes criterios:

Calificación	Descripción
Posible	Evento que nunca ha sucedido, pero se tiene la información que no descarta su ocurrencia
Probable	Evento ya ocurrido en el lugar o en unas condiciones similares
Inminente	Evento instrumentado o con información que lo hace evidente y detectable

De esta manera, una vez evaluada la probabilidad, se realiza el análisis de vulnerabilidad; entendida como la predisposición o susceptibilidad intrínseca que tiene la organización, a ser afectado o a sufrir pérdida, por la ocurrencia de la amenaza.

PASO 4. ESTIMAR EL IMPACTO

Se denomina impacto a la medida del daño, sobre el activo, derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Los tipos de impacto que se tienen son:

Impacto acumulado.
El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. Este es calculado sobre un activo teniendo en cuenta:

IR AL CONTENIDO

- Su valor acumulado (el propio más el acumulado de los activos que dependen de él).
- Las amenazas a las que está expuesto.

El impacto acumulado permite determinar las acciones a realizar para resguardar los activos y debe calcularse para cada activo y por cada amenaza.

Impacto repercutido.
El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. Este es calculado sobre un activo teniendo en cuenta:

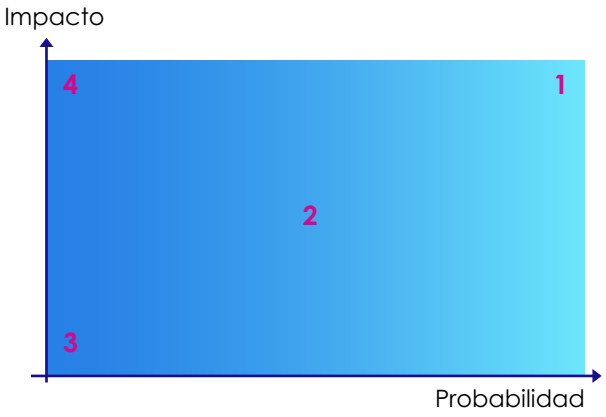
- Su valor propio.
- Las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido permite determinar las consecuencias de las incidencias técnicas existentes.

PASO 5. ESTIMAR EL RIESGO

Se denomina riesgo a la medida del daño probable sobre un activo. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo:

- Zona 1 – Riesgos muy probables y de muy alto impacto.
- Zona 2 – Riesgos probables de bajo impacto.
- Zona 3 – Riesgos improbables y de bajo impacto.
- Zona 4 – Riesgos improbables, pero de muy alto impacto.



Riesgo en función del impacto y la probabilidad[11]

Riesgo acumulado.
Es el calculado sobre un activo tomando en cuenta:

- El impacto acumulado sobre un activo debido a una amenaza.
- La probabilidad de la amenaza.

Riesgo repercutido.
Es el calculado sobre un activo tomando en cuenta:

- El impacto repercutido sobre un activo debido a una amenaza.
- La probabilidad de la amenaza.

11 Para su consulta: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

IR AL CONTENIDO

ANEXO 1. RECOMENDACIONES RESPECTO A AMENAZAS TÍPICAS

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

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

Tipo de amenaza	Amenazas	Posibles mecanismos de seguridad a implementar
Daño físico	• Fuego. • Agua. • Contaminación. • Accidentes. • Polvo, corrosión, humedad, congelamiento, radiación electromagnética. • Robo de soportes electrónicos. • Robo de información y/o soportes electrónicos.	• Adecuación de las instalaciones en las que se resguardan los activos. (mecanismo físico) • Traslado de activos a instalaciones que disminuyan la posibilidad de materialización de la amenaza. (mecanismo físico) • Generación de respaldos de información. (mecanismo físico y/o técnico y/o administrativo)
Eventos naturales	• Fenómenos climáticos o meteorológicos. • Fenómenos sísmicos. • Fenómenos volcánicos.	• Adecuación de las instalaciones en las que se resguardan los activos. (mecanismo físico) • Traslado de activos a instalaciones que disminuyan la posibilidad de materialización de la amenaza. (mecanismo físico) • Generación de respaldos de información. (mecanismo físico y/o técnico y/o administrativo)

IR AL CONTENIDO

Pérdida de servicios básicos	• Falla en el sistema de aire acondicionado o suministro de agua. • Pérdida de suministro eléctrico • Falla en los equipos de telecomunicaciones.	• Adecuación de las instalaciones en las que se resguardan los activos. (mecanismo físico) • Traslado de activos a instalaciones que disminuyan la posibilidad de materialización de la amenaza. (mecanismo físico) • Generación de respaldos de información. (mecanismo físico y/o técnico y/o administrativo) • Adecuación de la infraestructura para garantizar la continuidad del servicio. (mecanismo físico)
Información comprometida por fallas técnicas	• Intercepción e interferencia de señales. • Espionaje remoto. (escucha en comunicaciones) • Robo de medios o documentos. • Robo de equipo. • Recuperación de medios desechados o reciclados. • Revelación fuentes poco confiables para la obtención de datos. • Alteración de hardware. • Alteración de software. • Rastreo de localización. • Fallas del equipo. • Malfuncionamiento del equipo. • Saturación de los sistemas de información. • Malfuncionamiento del software. • Falla en el mantenimiento del sistema de información. – Ejecución de código malicioso. – Canales encubiertos y tráfico clandestino.	• Implementación de protocolos para el cifrado de la información. (mecanismo técnico y/o administrativo) • Generación de respaldos de información. (mecanismo físico y/o técnico y/o administrativo) • Implementación de servicios de seguridad a las instalaciones. (mecanismo físico y/o administrativo) • Implementación medidas de control de acceso a los activos. (mecanismo físico y/o administrativo) • Implementar restricciones para la instalación de software y hardware. (mecanismo físico y/o técnico y/o administrativo) • Acciones de revisión y mantenimiento y/o actualización de los equipos de cómputo. (mecanismo físico y/o técnico y/o administrativo) • Implementación de medidas de restricción para el uso de quipos de cómputo. (mecanismo físico y/o técnico y/o administrativo) • Actualización de la infraestructura de cómputo. (mecanismo técnico y/o administrativo)

IR AL CONTENIDO

Acciones no autorizadas	• Uso no autorizado de equipo. • Uso de software copiado o falsificado. • Abuso de privilegios por parte de los usuarios. • Consulta de información confidencial. • Suplantación de identidad. • Penetración y manipulación de los sistemas.	• Implementación de medidas de restricción para el uso de equipos de cómputo. (mecanismo físico y/o técnico y/o administrativo) • Implementar restricciones para la instalación de software y hardware. (mecanismo técnico y/o administrativo)
Compromiso de las funciones	• Error de uso. • Abuso de privilegios. • Falsificación de privilegios. • Denegación.	• Implementación de medidas de seguridad administrativas para la generación de perfiles de trabajo.

IR AL CONTENIDO

ANEXO 2. AMENAZAS POR ORIGEN

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

Origen de la amenaza	Motivación/causa	Posibles consecuencias
Hacker, cracker	• Desafío. • Dinero. • Ego. • Estatus. • Rebelión.	• Acceso no autorizado al sistema. • Ingeniería social. • Intrusión en los sistemas. • Robo de información.
Criminal computacional	• Alteración no autorizada de información. • Destrucción de información. • Ganancia económica. • Revelación ilegal de información.	• Acciones fraudulentas, robo. • Extorsión y chantaje, acoso. • Intrusión a los sistemas informáticos. • Sobornos de información. • Suplantación de identidad. • Venta de información personal.
Terrorista	• Chantaje. • Destrucción. • Explotación. • Ganancia política. • Reconocimiento mediático. • Venganza.	• Ataque a personas y/o instalaciones. (por ejemplo, bomba) • Ataque a sistemas. (por ejemplo, denegación de servicio) • Manipulación de los sistemas. • Penetración a los sistemas.

IR AL CONTENIDO

Espía industrial (inteligencia empresarial, gobiernos extranjeros, robo de tecnología, etc.)	• Espionaje económico. • Ventaja competitiva.	• Acceso no autorizado a información clasificada o propietaria. • Explotación económica. • Ingeniería social. • Intrusión a la privacidad del personal. • Penetración a los sistemas. • Robo de información. • Ventaja política.
Interno (Personal con poco entrenamiento, descontento, negligente, deshonesto o empleados despedidos)	• Curiosidad. • Ego. • Errores no intencionales u omisiones. (por ejemplo, errores de captura de información, errores de programación) • Ganancia económica. • Venganza.	• Abuso en la operación de los sistemas. • Acceso no autorizado a los sistemas. • Ataque a empleados y/o instalaciones. • Chantaje. • Código malicioso. • Consulta de información clasificada o propietaria. • Datos incorrectos o corruptos. • Errores en los sistemas. • Fraude y robo. • Intercepción de comunicaciones. • Intrusiones a sistemas. • Sabotaje de los sistemas. • Sobornos de información. • Venta de información personal.

IR AL CONTENIDO

BIBLIOGRAFÍA CONSULTADA

Diccionario de Protección de Datos Personales (Conceptos fundamentales).
https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProtec-cionDatosPersonales.pdf

Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Junio 2015.
https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

Recomendaciones para el manejo de incidentes de Seguridad de Datos Personales.
https://home.inai.org.mx/wp-content/uploads/Recomendaciones_Manejo_IS_DP.pdf

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.
https://d3t4nwcgmfrp9x.cloudfront.net/upload/AnalisisDeRiesgosRGPD.pdf

Gestión de riesgos, una guía de aproximación para el empresario.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguri-dad_gestion_riesgos_metad.pdf

Gestión de riesgo.
https://www.eird.org/cd/toolkit08/material/proteccion-infraestructura/gestion_de_riesgo_de_amenaza/8_gestion_de_riesgo.pdf

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