inai

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

RECOMENDACIONES para el Manejo de Incidentes de Seguridad de Datos Personales

(Sector Público)

Directorio

© **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales**
Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco,
C.P. 04530, Alcaldía Coyoacán, Ciudad de México.

Edición • Enero 2025

Contenido

1. Glosario

Las siguientes definiciones se retoman de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1], el Diccionario de Protección de Datos Personales[2], y la Guía de apoyo para la elaboración del documento de seguridad[3].

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

Activos críticos: Activos que un responsable considera como los más valiosos y que, sí ocurre su pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizada, podría provocar una crisis, y comprometer las operaciones, la prestación de servicios o incluso la existencia de la organización.

Alerta de seguridad: Hecho o evento que se detecta y/o registra en los sistemas de tratamiento físico o electrónico, el cual advierte de un posible incidente de seguridad.

Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.

Confidencialidad: Propiedad de la información para evitar su acceso, divulgación o revelación, no autorizados.

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.

Disponibilidad: Propiedad de la información para ser accesible y utilizable cuando se requiera.

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.

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

Incidente de seguridad: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la

[1] Para su consulta: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[2] Para su consulta: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

[3] Para su consulta: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf

integridad o la disponibilidad de la información.

Integridad: Propiedad de la información para salvaguardar la exactitud y completitud de la información.

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

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

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Responsable: En el sector público, de acuerdo con el artículo 3, fracción, XXXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos del ámbito federal, estatal y municipal, que decide sobre el tratamiento de datos personales (sujeto obligado).

Revelación o divulgación no autorizada: Exposición o manifestación de una verdad secreta u oculta[4]. Se trata de un incidente de seguridad donde se expone información que debía estar oculta sin autorización, perdiendo así la propiedad de confidencialidad[5].

Riesgo: Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño.

Sistema de tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

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,

[4] Definición obtenida del Diccionario de la Real Lengua Española. Disponible en https://dle.rae.es/revelaci%C3%B3n consultado el 31/10/2024.
[5] La legislación mexicana no define este concepto, sin embargo, en el Diccionario de Protección de Datos Personales. Conceptos Fundamentales, del INAI (Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf) se establece que la confidencialidad es un atributo de la información y al mismo tiempo un principio de seguridad que hace referencia a la obligación de que las personas que tienen acceso a ésta apliquen y respeten determinadas reglas y procedimientos a fin de que sea protegida de su divulgación no autorizada a terceros y se garantice que solo el personal autorizado pueda acceder a la misma, por lo que, interpretando a contrario sensu, la divulgación no autorizada es la pérdida de confidencialidad de información que debía mantenerse en secreto o inaccesible para ciertas personas.

conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Vulnerabilidad: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

Vulneración de seguridad: Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento. De acuerdo con el artículo 38 de la LGPDPPSO, se consideran al menos las siguientes vulneraciones: (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.

2. Introducción

Uno de los mayores retos a los que se enfrentan las entidades hoy en día, es planear y prepararse para lo inesperado, especialmente para los incidentes que comprometen los servicios que ofrecen, así como la información que resguarda el responsable, inclusive, los datos personales, poniendo en riesgo a su titular.

Alguno de los incidentes más comunes son los siguientes:

- Robo de información en documentos y medios de almacenamiento desechados incorrectamente.
- Empleados que acceden a datos personales sin la autorización correspondiente.
- Empleados que revelan información a otras personas a través de engaños.
- Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal.
- Acceso ilegal a las bases de datos personales por un externo a la organización.

> "La pregunta no es ***si ocurrirá el incidente***, sino ***cómo prevenirlo***"

Los incidentes de seguridad ocurren frecuentemente y pueden tener un gran impacto negativo en las instituciones. Por lo tanto, es imprescindible contar con medidas de seguridad para prevenir y mitigar dichos incidentes.

En México el derecho a la protección de datos personales se encuentra regulado por dos piezas legislativas, diferenciadas a partir de los sujetos a quien les resultan aplicables, es decir, una para el sector público y otra para el sector privado, en este documento, se abordara el contexto de la regulación para el sector público, el cual considera el cumplimiento al deber de seguridad; encaminando a que todo responsable del sector público que lleve a cabo un tratamiento de datos personales establezca medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra vulneraciones, lo cual permite identificar que toda violación a las mismas, constituye un incidente de seguridad con potencial a convertirse en una vulneración a la seguridad de los datos personales.

Por lo anterior, el INAI pone a disposición las presentes **Recomendaciones para el manejo de Incidentes de Seguridad de Datos Personales (Sector Público),** con el objeto de orientar a los responsables del sector público en el cumplimiento de las disposiciones vinculadas con la seguridad de los datos personales, en específico la atención y notificación de vulneraciones.

3. Objetivo

El objetivo de este documento es describir los procesos y controles recomendados por el Instituto para generar un plan de **respuesta a incidentes de seguridad, en particular para mitigar las vulneraciones a la seguridad de los datos personales.**

Estas recomendaciones ayudarán y orientarán a los responsables para lo siguiente:

1. **Reconocer** las diferencias entre alertas e incidentes de seguridad.
2. **Elaborar** un plan para responder ante incidentes de seguridad, conforme estándares internacionales.
3. **Utilizar** formatos de referencia para documentar los incidentes de seguridad.

4. Identificación de evento, incidente y vulneración a la seguridad de la información

Antes de iniciar con la descripción del proceso de respuesta a incidentes de seguridad, es necesario abordar una serie de conceptos base interrelacionados que son **activo, amenaza, riesgo, alerta, incidente, vulneración**.

Como se señaló en las definiciones, un activo es todo elemento de valor para una institución, 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 de amenazas, es decir, a factores externos que tienen el potencial de dañarlos, por ejemplo, una descarga eléctrica puede dañar un equipo de cómputo, o un empleado 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, por ejemplo, la descarga eléctrica sólo puede afectar a los equipos de cómputo que no tenga un regulador de voltaje. Por otro lado, el empleado podría acceder sin autorización a una base de datos si no está protegida con contraseña.

Los activos, las amenazas y las vulnerabilidades se combinan para generar **riesgos**[6] (Figura 1). **Cuando un riesgo se materializa, ocurre un incidente de seguridad**, el cual se traduce en una violación a las **medidas de seguridad**.

Figura 1. *Estructura de un riesgo*

> "Un incidente de seguridad es un riesgo materializado"

Para no confundir conceptos y entender de mejor manera a que se refiere cada elemento que interviene en la materialización de un incidente, es necesario definir y relacionar los siguientes conceptos:

[6] Para conocer más sobre el análisis de riesgos se puede consultar la Guía para implementar un sistema de gestión de seguridad de datos personales (Sector Público)https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf

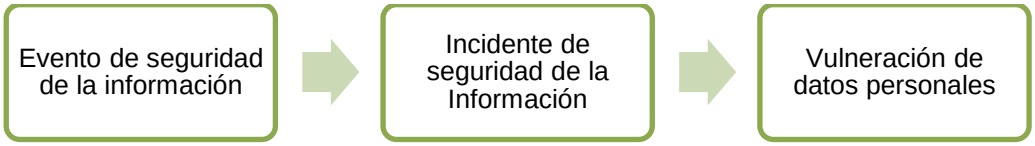

Figura 2. *Conceptos: evento, incidente y vulneración.*

A.Evento de seguridad de la información

Un evento de seguridad de la información se encuentra definido en el estándar internacional ISO/IEC 27002:2022[7] como *"un cambio en las operaciones diarias de una red o servicio tecnológico"*, es decir, de un sistema de tratamiento. Se trata de una ocurrencia observable que indica una posible infracción falla u omisión de por lo menos una medida de seguridad en alguno de los componentes del sistema de tratamiento de la información, sin embargo, no afecta negativamente a la operación de la institución.

Complementando esta definición, el estándar internacional ISO/IEC 27000:2018[8] define al evento de seguridad de la información *como "una ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad".*

Es así como, un evento a la seguridad al presentar un funcionamiento anómalo dispara una alerta que a su vez indica que existe la posibilidad de una falla en las medidas de seguridad, así como de intentos de ataques o fallos que descubren vulnerabilidades de seguridad existentes; dicha alerta implica que éste sea revisado para categorizarlo.

B.Incidente de seguridad de la información

La Guía para implementar un sistema de gestión de seguridad de datos personales (Sector Público)[9] define al incidente como *"el escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades"*. En otras palabras, un incidente es una amenaza para la seguridad de la información, lo cual deriva en un análisis del o los eventos de seguridad presentados a fin de identificar la posible violación de la seguridad de la información, lo cual puede comprometer la confidencialidad, integridad o disponibilidad de la información.

Es importante advertir que, un incidente no necesariamente afecta a los datos personales e incluso puede haber ocasiones en las que no impacte a las personas titulares de los datos personales.

Por ejemplo, de un empleado de una entidad, tras múltiples años de uso, deja de funcionar su equipo de cómputo por obsolescencia y no es posible recuperar toda la información en el almacenada, salvo cierta información que se encontraba respaldada en la nube, dicha información consta de cuestiones del negocio u organización que no contiene datos personales.

En este supuesto, estamos ante un incidente de seguridad que puede afectar la información posiblemente confidencial (sin tratarse de datos personales) ya que es posible que parte de esta no estuviese respaldada

[7] Definición obtenida del apartado 3.1.15 del estandar ISO/IEC 27002:2022, última consulta el 31 de octubre de 2024, disponible en: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27002:ed-3:v2:en

[8] Definición obtenida del apartado 3.30 del estandar ISO/IEC 27000: 2018, última consulta el 31 de octubre de 2024, Versión gratuita descargable en: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27000:ed-5:v1:en

[9] Guía para implementar un sistema de gestión de seguridad de datos personales (Sector Público): https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf

y no se pueda recuperar. En ese sentido, existe un incidente de seguridad que afecta negativamente a la institución, pero no transgrede datos personales ni a las personas titulares de estos.

Partiendo de lo anterior, un incidente de seguridad es un evento adverso o una violación a la seguridad de la información que puede comprometer la confidencialidad, integridad y/o disponibilidad de la información implícita o explícitamente, pero no necesariamente afecta a datos personales o a las personas titulares de datos personales.

C.Vulneración de datos personales

Este término debe entenderse como un incidente de seguridad de la información que afecta a los datos personales que posee el responsable del tratamiento, la particularidad de este concepto recae en la normativa en materia de protección de datos personales, ya que conforme a lo dispuesto en la LGPDPPSO se entienden como vulneraciones de seguridad a incidentes ocurridos en cualquier fase del tratamiento de datos personales.

El artículo 38 de la LGPDPPSO establece que las vulneraciones a la seguridad de los datos personales son al menos:

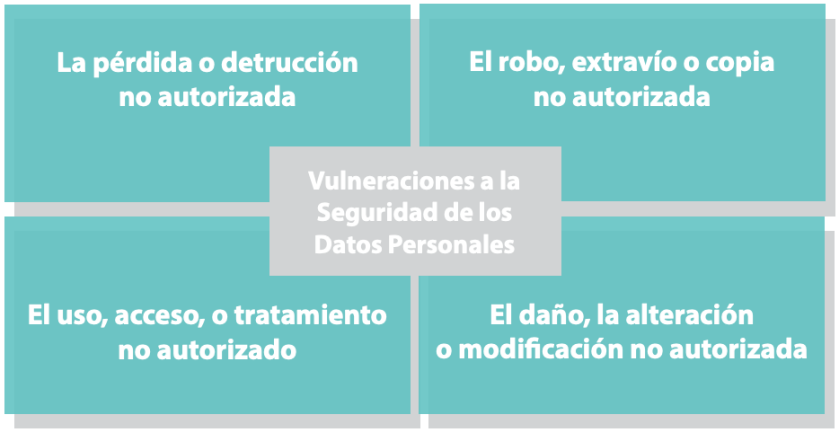

Figura 3. *Tipos de vulneraciones a la seguridad de los datos personales*

Es así que, para hablar de una vulneración, se debe partir de la identificación de un evento de seguridad de la información, que, tras su análisis, se torna un incidente por afectar a la institución, particularmente la confidencialidad, integridad y disponibilidad de la información, y, si, además, dicho incidente recae en alguno de los supuestos que precisa el artículo 38 de la LGPDPPSO, es decir, afecta a datos personales, nos encontramos ante un supuesto de vulneración de datos personales.

En resumen, la diferencia entre incidente y vulneración es que el primero es una transgresión a las medidas de seguridad en la organización que afecta a la confidencialidad, integridad o disponibilidad de la información, y una vulneración es un incidente que conlleva la pérdida, destrucción, robo, extravío, uso, acceso, tratamiento, daño, alteración y/o modificación no autorizada de datos personales. Por lo que podemos decir que toda vulneración de datos personales es un incidente de seguridad, más no todo incidente de seguridad es una vulneración de datos personales.

> "Las vulneraciones a la seguridad
> de los datos personales son incidentes de seguridad"

De esta manera, es posible observar que las vulneraciones de seguridad son incidentes de seguridad que involucran datos personales, las cuales podrían resultar en revelaciones de información, como se muestra en la figura siguiente:

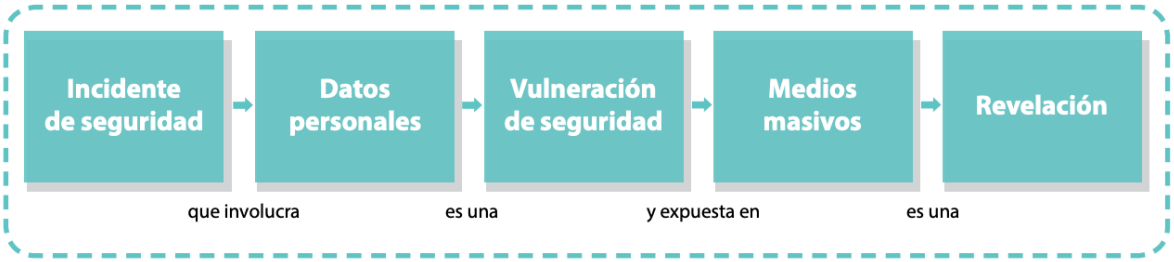

Figura 4. *Incidentes de seguridad que comprometen datos personales*

Las vulneraciones a la seguridad de los datos personales o vulneraciones de seguridad mencionadas en el artículo 40 de la LGPDPPSO, **son un tipo particular de incidente de seguridad** que se caracterizan por:

a) Afectar a los activos o sistemas relacionados con los datos personales, en cualquier fase de su tratamiento, y
b) Afectar de manera significativa los derechos patrimoniales o morales de las personas titulares de los datos personales.

Un ejemplo de incidente de seguridad que conlleva una vulneración de datos personales son las **revelaciones o divulgaciones no autorizadas de datos personales;** es decir, se **expone la información a través de Internet o en medios de comunicación masivos.**

En este ejemplo, además de transgredir la seguridad de la información, se transgrede el derecho a la protección de datos personales de personas titulares, y particularmente el deber de confidencialidad que tiene la entidad responsable del tratamiento de datos personales[10].

En ese contexto, derivado de una vulneración de seguridad, los responsables del tratamiento tienen obligaciones diversas que serán listadas y desarrolladas en los siguientes apartados, pero en principio tienen el deber de analizar las causas por las cuales se presentó ésta y desplegar acciones correctivas para de ser posible, intentar detener el incidente, o bien gestionar los efectos negativos de este, e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar **las medidas de seguridad para evitar que incidentes similares se repitan**[11].

Continuando con el ejemplo, cuando se identifica que una divulgación no autorizada de información expone datos personales, el responsable debe tomar todas las medidas que estén a su alcance para mitigar la difusión o publicación de estos. Por ejemplo, solicitar la baja de contenido al administrador de una página web, así como pedir la eliminación de resultados de un motor de búsqueda, a fin de minimizar el daño a las

[10] Se sugiere la lectura de las Recomendaciones de para el cumplimiento del deber de confidencialidad. Disponible en: https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/Recomendaciones_Deber_Confidencialidad.pdf
[11] De acuerdo al artículo 37 de la LGPDPPSO.

personas titulares.

Como se mencionó anteriormente, los responsables tienen ciertas obligaciones que cumplir conforme al marco normativo, que para el sector público identifica:

a) Elaborar una bitácora de vulneración de datos personales.[12]
b) Informar a las personas titulares de los datos personales afectados.
c) Informar al INAI o al organismo garante de la Entidad Federativa correspondiente de la vulneración de seguridad ocurrida.

[12] Artículo 39 de la LGPDPPSO.

5. Bitácora de vulneraciones

Una bitácora[13] es una herramienta de trabajo diseñada para que, a través de la información escrita en ella, se haga una descripción breve, concreta, sencilla y entendible de todos los eventos relevantes ocurridos durante la ejecución de una tarea, estableciendo que los eventos que se especifican en esta son aquellos que rompen con la normalidad de la ejecución de la tarea, lo que podría indicar un evento adverso que puede llegar a comprometer la seguridad de la información.

Como se precisó en el apartado anterior, la elaboración de una bitácora de vulneraciones de datos personales es obligatoria para los responsables del tratamiento del sector público, de conformidad con el artículo 39 de la LGPDPPSO, toda vez que es una herramienta muy útil de análisis y prevención de riegos que puede aportar a la mejora continua del sistema de gestión de seguridad de datos personales.

De acuerdo con el precepto señalado, la bitácora al menos debe contener:

1. La descripción de la vulneración
2. La fecha en la que ocurrió
3. El motivo que originó la vulneración
4. Las acciones correctivas implementadas de forma inmediata y definitiva.

No obstante, se sugiere que todo incidente de seguridad sea vulneración de datos personales o no, se describa en la bitácora, puesto que, en ocasiones, el que un incidente comprometa datos personales puede ser una cuestión fortuita. En ese sentido, si se comienza a trabajar la bitácora en cuanto sucede el evento y se procede a su categorización, ya se tendrá avanzado el análisis y la descripción del incidente, lo que se traduce en tiempo ganado para el restablecimiento de la organización.

Previo a la elaboración de una bitácora es importante establecer quienes intervendrán en el llenado y actualización de la bitácora, así como definir sus contenidos, los cuales como mínimo deben contener lo señalado por el artículo 39 de la LGPDPPSO, aunque estos se pueden ajustar a las necesidades y contextos de los responsables.

Podrá consultar una propuesta de bitácora en el Anexo correspondiente de las presentes recomendaciones.

> “La seguridad es un proceso constante, en la medida en que se documente, evalúe y analice lo que pasa alrededor del tratamiento, se podrá enfrentar de mejor manera los riesgos, aquí radica la importancia de la bitácora”.

[13] Definición de bitácora obtenida del sitio web: https://concepto.de/bitacora/, última consulta del 31 de octubre de 2024

5. Equipo de respuesta a incidentes

El Equipo de Respuesta a incidentes no es una figura que contemple el marco normativo en materia de protección de datos personales; sin embargo, es una figura importante dentro de las recomendaciones y estándares enfocados a la atención de incidentes cibernéticos y no cibernéticos.

Por lo que, podemos establecer que es una buena práctica asignar roles[14] en función de la estructura interna de cada responsable, será necesario que su inclusión se vincule con los posibles actores que podrían llevar a cabo este tipo de respuesta.

Por ejemplo, considerar a la Unidad de Transparencia incluido el Oficial de Protección Datos Personales, en su caso, en conjunto con la Dirección de Tecnologías de la Información, Dirección Informática o similares en su caso, como las áreas que podrían apoyar a las demás unidades administrativas para atender y dar seguimiento a incidentes de seguridad y vulneraciones de seguridad de datos personales dentro del sujeto obligado.

Un equipo de respuesta a incidentes de acuerdo con el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos[15], de Presidencia de la República de México, define a este como *"un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas con la finalidad de mitigar sus acciones y efectos, y restaurar las condiciones normales de operación"*[16].

El objetivo de dicho equipo es el de proveer a la institución de una capacidad apropiada para evaluar, responder y aprender de los incidentes de seguridad de la información.

La composición de dicho equipo requiere definir perfiles para conjuntar un equipo multidisciplinario con personal técnico y no técnico, si bien, es necesaria la presencia de especialistas en seguridad de la información, los cuales serán responsables de la gestión de incidentes de seguridad, también es importante contar con un equipo complementario que incluya las áreas jurídicas y de administración de personal, es así que, este equipo puede estructurarse de diferentes formas en una organización de acuerdo con el tamaño, personal y al tipo de industria al que pertenece la entidad.

Conforme con la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[17] específicamente para atención de incidentes informáticos, este equipo *"presta los servicios necesarios para ocuparse de estos incidentes y ayuda a los clientes del grupo al que atienden a recuperarse después de sufrir uno de ellos"*.

De manera genérica, se puede integrar al equipo por niveles de atención:

- Personal que identifica los eventos a la seguridad
- Personal técnico y no técnico al que se le escalan los incidentes de seguridad
- Personal especialista que coordina los trabajos

Las actividades que realiza este equipo están ligadas directamente al ciclo de vida de la respuesta a

[14] De acuerdo con los artículos 33, fracción II y 35 fracción III de la LGPDPPSO, así como 57 de los Lineamientos Generales, se debe recordar que para la implementación de un Sistema de Gestión de Datos Personales y para la elaboración del Documento de Seguridad, se deben definir las funciones y obligaciones del personal que trata datos personales, los roles y responsabilidades particulares, para así definir la cadena de rendición de cuentas.
[15] Presidencia de la República, Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. Octubre 2021 última consulta el 31 de octubre de 2024. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf
[16] Ibidem, p. 41.
[17] ENISA, Cómo crear un Csirt Paso a Paso. última consulta el 31 de octubre de 2024, disponible en: CSIRT Setting up Guide in Spanish— ENISA (europa.eu)

incidentes que está homologado con el estándar NIST 800-61[18], por lo que, deberá:

- Determinar y proporcionar políticas, servicios e instrucciones de respuesta para los incidentes de seguridad.
- Informar apropiadamente sobre los incidentes que han sido detectados.
- Manipular (identificar, contener y erradicar) correctamente el incidente.
- Reaccionar rápidamente a las amenazas, infracciones y los ataques para minimizar los daños y reducir el costo de recuperación.
- Realizar una investigación profunda sobre el incidente ocurrido, a fin de conocer que origino el incidente y contar con evidencia suficiente para los pasos posteriores.
- Trabajar en las lecciones aprendidas que ayuden a evitar la materialización del mismo incidente.

Particularmente, los servicios generalmente se asocian en:

I. Servicios reactivos: es decir, aquellos que se inician ante un evento o a solicitud de algún involucrado en el sistema de tratamiento.
II. Servicios proactivos, que son aquellos que brindan asistencia e información para ayudar a resguardar y preservar los sistemas y componentes tecnológicos ante futuros ataques; y
III. Los servicios de gestión de calidad, que son aquellos que asisten indirectamente a disminuir la cantidad de incidentes.

[18] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, capitulo 2, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

6. Gestión de incidentes de seguridad

La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Por lo tanto, **elaborar un plan de respuesta a incidentes es probablemente una de las tareas más complejas en seguridad de la información.**

Por lo anterior, es importante que se consideren todas y cada una de las etapas del ciclo de vida de las respuestas a incidentes, previsto en el Estándar NIST 800-61[19]. Por lo anterior, a través de este apartado se **ofrecerán recomendaciones para atender incidentes de seguridad,** a fin de prevenir y mitigar las vulneraciones a la seguridad de los datos personales.

Figura 5. *Imagen del ciclo de respuesta a incidentes propuesto en NIST 800-61*

Para ello antes de abordar el esquema general, es necesario definir el ciclo que detona en la identificación del incidente, es decir, los resultados del monitoreo de las medidas de seguridad que advierten un potencial incidente de alertas de seguridad.

A. Alertas e incidentes de seguridad

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento.

Es importante considerar que las alertas de seguridad pueden presentarse desde factores externos y factores internos.

- En el caso de los factores externos, por ejemplo, a través de una noticia en medios de comunicación, de un aviso por parte de un ente externo al responsable, o a través de una denuncia.
- En el caso de los factores internos, a través de los mecanismos de monitoreo o investigación interna que tenga establecido el responsable.

[19] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, figura 3-1, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Sin embargo, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte.

A continuación, se presenta una lista de alertas de seguridad, que pueden advertir de una anomalía o cambio no deseado en los activos:

Ejemplos de alertas de seguridad	
Entorno	**Tipo de alerta**
Físico	Alarmas para desastres como incendios o terremotos.
	Alarmas automatizadas contra robos o intrusos en instalaciones.
	Alertas del personal de vigilancia o a través de circuito cerrado de video.
	Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos.
	Avisos del personal, clientes, proveedores, autoridades o reportes en medios de comunicación masivos.
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físicos.

Ejemplos de alertas de seguridad	
Entorno	**Tipo de alerta**
Electrónico	Notificaciones sobre software malicioso o vulnerabilidades técnicas descubiertas, preferentemente de fuentes confiables como agencias nacionales o firmas especializadas en riesgos o seguridad.
	Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos (IDS, por sus siglas en inglés) o gestores de seguridad de la información y eventos (SIEM, por sus siglas en inglés).
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo.

Tomando como referencia la tabla anterior, las alertas de seguridad pueden ser manuales o automatizadas, y originarse a través de distintas fuentes, entre las más comunes están:

a) Clientes o titulares de los datos personales.
b) Usuarios de los sistemas de tratamiento.
c) Subcontrataciones.
d) Departamentos de tecnologías de la información internos o de proveedores.
e) Departamento de datos personales.
f) Mesa de servicio o departamentos de atención al cliente.
g) Proveedores de servicios de telecomunicaciones e Internet.
h) Unidades de negocio.
i) Medios de comunicación masivos, y
j) Sitios web especializados.

Por ejemplo, derivado de la queja de una persona titular, un responsable podría enterarse que los datos personales de sus usuarios se están utilizando por un tercero no autorizado. O bien, que una institución se entere de que sus sistemas de tratamiento han sido comprometidos o *hackeados*, a través de una

publicación en medios de comunicación masivos.

Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos, se habla de **un incidente de seguridad**.

En la siguiente tabla se enlistan diferentes categorías de incidentes de seguridad:

Ejemplos de alertas de seguridad	
Categoría	**Ejemplos**
Desastre natural (más allá del control humano)	Terremoto, erupción de un volcán, tsunami, huracán, etcétera.
Inestabilidad social	Huelgas, terrorismo, guerra.
Daño físico (accidental o deliberado)	Incendio, inundación, malas condiciones ambientales (contaminación, polvo, corrosión, congelamiento), radiación o pulso electromagnético, destrucción parcial o toral de medios de almacenamiento físico o electrónico.
Falla de la infraestructura	Falla en el suministro de servicios como: energía, agua, telecomunicaciones y redes, aire acondicionado.
Falla técnica	Fallas del hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento.
Software malicioso[20]	Diferentes categorías de software malicioso (malware) como virus, troyanos, software de acceso y control remoto (RAT, por sus siglas en inglés), amenazas persistentes avanzadas (APT, por sus siglas en inglés), Ransomware.
Ataques técnicos	Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a la fuerza y escaneo de redes, utilización de puertas traseras en el software, intentos de acceso no autorizado, inferencia de contraseñas, ataques de denegación de servicio.
Incumplimiento de reglas o políticas (accidental o deliberado)	Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas o ilegales, copia o sustracción de documentos o información no autorizada.
Información dañada	Sobre escritura accidental, error de captura o de almacenamiento.
Intercepción de información	Espionaje, intervención de comunicaciones, ingeniería social, robo, pérdida o extravío de información.
Divulgación de contenido perjudicial	Difusión en medios de comunicación masivos de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas.

En suma, **un riesgo materializado es un incidente, y se detecta a través de las alertas de seguridad**,como se puede observar en la figura siguiente:

[20] En el Anexo 3 de este documento se desarrollan recomendaciones para que los usuarios se protejan contra el software malicioso, más allá de las premisas de la institución, y así minimizar incidentes de seguridad en los sistemas de tratamiento.

Figura 6. *Relación entre riesgos, incidentes y alertas de seguridad.*

B. Etapas del plan de respuesta a incidentes de seguridad

El plan de respuesta a incidentes parte de la gestión de incidentes, la cual es un proceso cíclico mediante el cual una institución responde y maneja un incidente empleando procedimientos establecidos para trabajar con los incidentes ocurridos.

El objetivo principal de contar con un esquema de gestión de incidentes de seguridad de la información es proporcionar documentación detallada que describa las actividades y procedimientos para tratar los eventos e incidentes y comunicarlos en el momento oportuno. El esquema de gestión de incidentes de seguridad de la información entra en efecto siempre que se detecte un evento de seguridad de la información o se reporte una vulnerabilidad de seguridad de la información

A continuación, se desarrollan las **siete etapas** mínimas las cuales son estandarizadas y parten del documento NIST800-61[21] para generar y documentar un plan de respuesta a incidentes. El plan de respuesta a incidentes se enfoca en la mejora continua, a través de estándares internacionales en la materia y de innovaciones tecnológicas.

1. Preparación

El objetivo de esta etapa es **desarrollar y mantener políticas, controles de seguridad y otros mecanismos que permitan actuar ante los incidentes de seguridad** planteados anteriormente.

> "El plan de respuesta a incidentes requiere de medidas de seguridad previamente implementadas"

La preparación a los incidentes está directamente relacionada con la implementación de un Sistema de Gestión de Seguridad de Datos Personales[22].

Particularmente en la elaboración de políticas y protocolos que se pueden iniciar en la fase de planeación del propio sistema, y que se implementa en las siguientes fases. Es así como, contar con un Sistema de Gestión, brindará elementos que son necesarios en cada etapa que involucra la gestión del incidente, como lo es identificar los activos en los sistemas de tratamiento, así como los riesgos y medidas de seguridad existentes.

[21] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, Incident Response Life Cycle, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[22] Se puede consultar la Guía para implementar un sistema de gestión de seguridad de datos personales (Sector Público) https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/GuiaSGSDP_sectorpublico.pdf

Sin embargo, si no se cuenta con un sistema de gestión u otro proceso para la mejora continua de las medidas de seguridad, al menos se deben identificar los elementos que servirán como base del plan de respuesta, en caso de que se presente un incidente de seguridad.

Se debe recordar que la implementación de un Sistema de Gestión de Seguridad de Datos Personales es obligatorio para los responsables del tratamiento del sector público, de conformidad con el artículo 34 de la LGPDPPSO.

De acuerdo con el apartado de preparación del documento NIST 800-61[23] *"la preparación generalmente se divide en prevenir incidentes y preparase para manejar los incidentes, identificando que, esta actividad no solo permite (i) establecer la capacidad de respuesta a incidentes para que la organización esté lista para responder a estos, sino también (ii) dota de un mecanismo que asegura la seguridad de la información en los activos involucrados en el sistema de tratamiento".*

Es así como, complementando la preparación, se debe entender el alcance de un equipo de respuesta a incidentes, el cual conforme al documento previamente citado establece que *"Está fuera del alcance de las recomendaciones brindar asesoramiento específico sobre cómo proteger redes, sistemas y aplicaciones. Aunque los equipos de respuesta a incidentes generalmente no son responsables de proteger los recursos, pueden defender prácticas de seguridad sólidas."*[24].

En concordancia con lo anterior, conforme a la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia[25], *"la etapa de preparación debe ser apoyada por un área de tecnologías de la información o quien haga sus veces para el aseguramiento de redes, sistemas, y aplicaciones informáticas en donde se procese la información."*

Esta etapa requiere de una serie de actividades para afrontar las demás etapas, por lo que, es necesario considerar al menos lo siguiente:

- Formular y producir una política de gestión de incidentes de seguridad.
- Definir y documentar un plan detallado de gestión de incidentes de seguridad de información.
- Establecer un equipo de respuesta a incidentes de seguridad.
- Identificar los activos en los sistemas de tratamiento, así como los riesgos y medidas de seguridad existentes.

El inventario de activos para el sector público es parte del contenido del sistema de gestión de seguridad de datos personales y el documento de seguridad; este es importante para identificar los siguientes elementos que servirán como base del plan de respuesta, en caso de que se presente un incidente de seguridad, a saber:

- Los activos que son relevantes para la institución.
- Las medidas de seguridad que tienen los activos.
- Las alertas de seguridad, asociadas con dichas medidas o controles.
- Los propósitos de las medidas de seguridad para mitigar un incidente.

[23] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.1 Preparation, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[24] Ibidem, p. 23.
[25] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Técnologías de la Información y las Comunicaciones de Colombia, última consulta el 31 de octubre de 2024. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Por ejemplo, para una entidad que tiene bases de datos en computadoras conectadas a Internet, una lista sencilla con los elementos mencionados anteriormente podría verse así:

Inventario de preparación			
Activo	**Medida de Seguridad**	**Alerta de Seguridad**	**Propósito de la medida de seguridad ante un Incidente**
Base de datos automatizada de las personas titulares	Copia mensual de la base de datos en un medio de almacenamiento externo	No aplica. El respaldo por sí mismo no proporciona alertas.	Se puede usar la copia de la base de datos en caso de robo, pérdida o extravío de la base de datos principal.
	Antivirus	Alerta si el archivo se encuentra infectado o dañado.	El antivirus notifica al usuario de la falla en el archivo. El antivirus puede intentar reparar el archivo dañado.
Equipo de cómputo	Bloqueo con contraseña	Alerta si se han sobrepasado el número de intentos de acceso.	Bloquea el equipo en caso de que se sobrepasen los intentos de acceso.
	Guardia de seguridad	Alerta si el equipo de cómputo ha sido sustraído sin autorización.	Iniciar la investigación respecto al activo desaparecido.

La tabla desarrollada anteriormente permite conocer:

a) La relación que existe entre los activos, sus medidas de seguridad, las alertas que se proporcionan a través de dichas medidas, y su propósito, a fin de mitigar un incidente de seguridad.
b) Los activos desprotegidos o carentes de medidas de seguridad para mitigar un incidente.

La fase de preparación consiste en identificar e implantar **medidas de seguridad, mientras no se presente un incidente**, por ello se recomienda la implementación de un sistema de gestión que permita la mejora continua de la seguridad en una institución. Algunas de las medidas de seguridad y acciones relevantes para la preparación son:

- **RESPALDOS O COPIAS DE SEGURIDAD**

La creación de respaldos o copias de seguridad es una medida particularmente importante, ya que permite a las instituciones recuperar la información dañada, robada o destruida, así como recobrar la operación normal de sus sistemas de tratamiento, en otras palabras, se lleva a cabo lo siguiente:

- La recuperación de archivos o documentos.
- La restauración completa de sistemas de tratamiento.

Es importante determinar el o los tipos de respaldo necesarios para una institución, ya que un exceso de respaldos podría consumir tiempo y recursos, pero una falta de ellos podría dificultar la recuperación en caso de un incidente.

Un respaldo no siempre representa una copia idéntica de todo el contenido de un equipo de cómputo o sistema de tratamiento, sino de los datos necesarios para el adecuado uso de la información.

De este modo, es posible identificar tres tipos principales de respaldo:

1. **Respaldos completos:** Se realiza una copia completa del archivo o medio de almacenamiento. Es decir, si se tienen los archivos 1, 2 y 3, se copian todos sin importar su fecha de modificación o creación. Un respaldo completo no se debería realizar frecuentemente por la cantidad de recursos que puede llegar a consumir.
2. **Respaldos incrementales:** Sólo se realiza copia de la información que ha sido modificada desde el último respaldo. Es decir, si se tienen los archivos 1, 2 y 3, y desde el último respaldo sólo se modificó el archivo 3, este es el único que se respalda, porque ya hay una copia de los archivos 1 y 2. Los respaldos incrementales se utilizan en conjunto con los respaldos completos para optimizar el uso de recursos, sin embargo, puede ocurrir que, para encontrar un archivo, se tenga que pasar por un respaldo completo y varios respaldos incrementales.
3. **Respaldos diferenciales:** Son similares a los respaldos incrementales en cuanto a realizar la copia de los archivos que han sido modificados desde el último respaldo; sin embargo, estos respaldos se caracterizan por ser acumulativos, es decir cuando se actualiza un archivo, se actualiza en todos los respaldos existentes.

   Los respaldos se pueden realizar a documentos físicos, sistemas operativos, software y aplicaciones, bases de datos, o datos de usuario.

   Para la realización de respaldos se puede optar por la copia manual, o bien valerse de sistemas automatizados, considerando los siguientes puntos:
   - Planificar la periodicidad con la que se realizarán los respaldos.
   - Considerar dónde se resguardarán, cómo se actualizarán y cómo se eliminarán.
   - Hacer pruebas periódicas de que los respaldos funcionan, y así garantizar que serán de utilidad en caso de un incidente.

Para los medios de almacenamiento en formato físico, además de hacer copias simples, se recomienda optar por la digitalización de los documentos y archivos.

• ELEMENTOS PARA LA RESPUESTA A INCIDENTES

Cuando el tamaño de la Institución lo permita, la gestión de incidentes se deberá asignar a un equipo o área que deberá contar con políticas específicas, acceso a los activos y herramientas para el monitoreo y atención de las alertas de seguridad. En el Anexo correspondiente se encuentra el formato de lista de contactos, que se puede utilizar para identificar a los posibles involucrados en la atención de un incidente de seguridad.

Debido a que **las organizaciones pequeñas** podrían carecer del conocimiento o de las áreas técnicas requeridas para investigar incidentes de seguridad complejos, se recomienda que centren sus esfuerzos en la **creación y prueba de copias de seguridad de sus activos críticos**, a fin de mantener al menos la capacidad de regresar a sus operaciones normales.

Por ejemplo, de todos los sistemas de información de una entidad, si se vulneran activos críticos como las bases que contienen datos personales, se pierde la capacidad de responder a las solicitudes de derechos de acceso, rectificación, cancelación y oposición, que establece la normativa en protección de datos personales, lo que puede tener consecuencias para el responsable, tales como: sanciones, daño reputacional y, en ocasiones, la pérdida de clientes o usuarios.

De manera general, algunos de los controles que se deben establecer para la gestión de incidentes son:

Políticas: que respalden la creación y el funcionamiento del equipo de respuesta a incidentes.

Elaboración del plan o estrategia: dependiendo de los mecanismos para detectar alertas de seguridad, se debe establecer una cadena de atención, revisión y aprobación de la mitigación de posibles incidentes de seguridad.

Comunicación: Durante cualquier etapa de la atención de un incidente, se debe mantener comunicación entre los miembros del equipo de respuesta, y otras partes interesadas como la alta gerencia o autoridades.

Documentación: Se deberá establecer un proceso y los formatos necesarios para documentar cada descubrimiento o acción realizada en atención a un incidente de seguridad. Es importante que esta documentación considere un almacenamiento ordenado y sistemático, que responda al qué, cómo, cuándo, dónde, y porqué de los incidentes de seguridad atendidos. Para mayor referencia, en el Anexo correspondiente de este documento se encuentran los formatos para la respuesta a un incidente.

Control de acceso: El equipo de respuesta a incidentes debe de contar con las credenciales necesarias para tener acceso a cualquier activo involucrado en un incidente de seguridad. Es importante mencionar que, dependiendo del tipo de activo, el nivel de acceso deberá estar restringido al grado de conocimiento técnico para extraer información sobre el incidente. Por ejemplo, el administrador de redes debería ser la persona designada para apoyar con las alertas de seguridad en un equipo de cómputo, mientras que eljefe de archivos debería ser el encargado de documentar la falta de un expediente físico.

Herramientas: Es altamente recomendable tener hardware y software destinados a atender una alerta de seguridad, y comenzar la mitigación en caso de confirmar un incidente. Dependiendo de los activos del responsable, y de las medidas de seguridad existentes, estas herramientas pueden incluir de manera enunciativa, más no limitativa, los siguientes elementos: antivirus portátiles, discos duros y memorias USB, software para analizar tráfico de red, así como, desarmadores y pinzas. Además, se pueden tener listas de revisión generales, como la que se proporciona en el apartado **Lista de revisión para la respuesta a incidentes**, y algunas listas específicas con comandos a ejecutar para sistemas operativos y herramientas.[26]

La mochila de respuesta a incidentes

La mochila de respuesta (jump bag) es un concepto comúnmente usado sobre las herramientas que se deben tener a la mano para atender una alerta o incidente de seguridad.

Se recomienda que esta mochila esté a la mano de cada uno de los integrantes del equipo de respuesta a incidentes y que contenga, de manera ordenada, al menos lo siguiente:

- Un diario, libreta, bitácora o formatos en blanco, así como plumas y lápices, para documentar el que cómo, cuándo, dónde y quiénes están involucrados en una alerta o incidente de seguridad.
- La lista de contactos del equipo de respuesta a incidentes.
- Medios de almacenamiento o memorias USB sin información, en su caso, borrados con métodos

[26] Por ejemplo, el Instituto SANS ofrece dentro de su apartado de descargas, trípticos y listas rápidas ("Cheat Sheats") para revisar las bitácoras de sistemas operativos, o bien ejecutar comandos en herramientas de software. Véase: https://pen- testing.sans.org/resources/downloads

seguros, y listos para usarse

- Una memoria USB o un **disco** compacto (boot cd) con un sistema operativo ejecutable desde arranque, el cual contenga exclusivamente antivirus y herramientas de software para la revisión.
- Una computadora portátil dedicada exclusivamente a la respuesta a incidentes, con capacidad de conexión a Internet y únicamente con las aplicaciones, credenciales y configuraciones necesarias ya pre-cargadas y funcionales.
- Herramientas para agregar o quitar dispositivos de la conexión física a redes, así como los cables correspondientes.
- Cámara fotográfica con datos de ubicación, fecha y hora debidamente configurados, para contar con imágenes del incidente.
- Cuando se cuenta con el servicio subcontratado, o áreas técnicas especializadas en la investigación forense digital, la mochila deberá contar con:
    - Equipo de protección contra escritura.
    - Software y/o hardware para generar imágenes forenses[27]
    - Guantes de látex.
    - Bolsas de plástico, preferentemente anti-estática.

Es importante aclarar que ninguno de los artículos de la mochila debe contener datos personales o información reservada o confidencial de la entidad, más que la estrictamente necesaria para su propio uso.

En ninguna circunstancia, la mochila debe estar al alcance de personas ajenas al equipo de respuesta a incidentes. Asimismo, ninguno de los artículos de la mochila deberá utilizarse para un fin distinto a la respuesta a incidentes.

La mochila de respuesta a incidentes hace las veces de un botiquín, y se debe renovar y recargar después de cada uso o de manera previa si es necesario para considerar las actualizaciones pertinentes.

Entrenamiento: Las instituciones con equipos de respuesta a incidentes deben optar por proporcionar a su personal el debido entrenamiento, ya que conforme los sistemas de tratamiento se vuelven más complejos, éstos contienen más información y es común detectar un incremento en la ocurrencia de alertas de seguridad.

"Entre más automatizado y complejo es un sistema de tratamiento, mejor entrenado debe estar el personal que lo maneja"

2. Detección/Identificación

En esta etapa **se detectan los indicadores respecto a la seguridad de la información y se determina si se encuentra frente a un incidente**, de acuerdo con el estándar NIST 800-62[28] se denomina indicador a cualquier evento que cuente con la probabilidad de traducirse en un incidente, lo cual puede ser identificado de muchas fuentes diferentes como lo son:

[27] La imagen forense es una copia exacta del contenido de un medio de almacenamiento electrónico, y sirve como evidencia para realizar una investigación digital de una alerta o incidente

[28] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.2.2 signs of an incident, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- Alertas de seguridad.
- Alertas de seguridad web.
- Una amenaza directa de un grupo especifico.
- Activaciones de sensores de detección de intrusos.
- Alertas de software antivirus.
- Alertas de softwares especializado.
- Registros de usuarios.
- Funcionamientos anómalos que no son registrados en una alerta.
- Información disponible públicamente.

La detección e identificación debe proporcionar suficiente información para que el equipo priorice las actividades posteriores como la contención del incidente y un análisis más profundo de sus efectos.

Es así como, esta fase involucra una actividad denominada monitoreo de medidas de seguridad, por lo que, es necesario saber cómo se revisa el funcionamiento de las medidas de seguridad, ya que, es el parámetro inicial que nos indica un funcionamiento anómalo en el tratamiento de la información, esta información debería estar contenida en el apartado de mecanismos de monitoreo y revisión de su documento de seguridad.

El monitoreo de las medidas de seguridad permite conocer eventos adversos para que sean analizados a fin de catalogarlos como incidentes, por lo que, se puede determinar que un evento no siempre es un indicador de un incidente, para llegar a esa determinación es necesario contar con información que dé cuenta sobre una afectación a los activos, estableciendo que entre más información se pueda recabar, existirá mayor certeza respecto al incidente.

De esta manera, en esta fase, los eventos y vulnerabilidades requieren haber sido clasificados como incidentes de seguridad. Para esta fase, se debe de emprender el desarrollo de las siguientes actividades:

- Realizar un seguimiento y registrar las actividades de los mecanismos de monitoreo y revisión implementados.
- Detectar e informar la ocurrencia de un evento de seguridad o la existencia de una vulnerabilidad de seguridad, ya sea de forma manual por el personal que opera el sistema de tratamiento o automatizada a través de un mecanismo.
- Recopilar información sobre una vulnerabilidad o evento de seguridad de la información.
- Garantizar que todas las actividades, resultados y las decisiones relacionadas son registradas apropiadamente para su posterior análisis.
- Garantizar la generación de evidencia para obtener información detallada sobre el incidente.

Toda la información recolectada relacionada con un evento de seguridad de información o un incidente se debe almacenar en una bitácora, la cual se recomienda sea gestionada por el equipo de respuesta a incidentes, además de que al menos dos personas estén involucradas en la identificación de un incidente, una para evaluar el incidente e identificar activos que pudieran ser afectados, y otra dedicada a documentar y recabar evidencia.

Es importante indicar que, en ocasiones por su naturaleza, las alertas reflejan un incidente de manera evidente, y por lo tanto no requieren una investigación intensiva para pasar a la fase de contención. Por ejemplo, un evento en el que un empleado que de manera accidental derrama el café sobre documentos o equipo de cómputo, se puede catalogar de manera inmediata como un incidente.

Sin embargo, una vez que se identifica un incidente, siempre es necesario buscar alertas adicionales a la

que detonó la identificación, para determinar su alcance total. Por ejemplo, derivado de una auditoría se tiene conocimiento que se han extraviado los expedientes en papel de un grupo de pacientes, esto ya es un evento que se puede catalogar como incidente; no obstante, se tendría que realizar una revisión en el archivo a fin de identificar si otros expedientes han sido sustraídos.

Se puede utilizar el formato de identificación de incidentes del Anexo correspondiente para documentar una o más alertas que se consideren relevantes o que se relacionen con un incidente de seguridad.

3. Análisis

Esta fase requiere la confirmación de la detección de que el o los eventos de seguridad ya son catalogados como incidentes a la seguridad de la información, por lo que, es necesario recopilar información para tomar decisiones sobre el incidente. Para ello podrá seguir la siguiente ruta:

A. Evaluación

La etapa de evaluación de acuerdo con la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información[29] del Ministerio de Tecnologías de la Información y Comunicaciones sugiere que *"para realizar la evaluación de un incidente a partir los niveles de impacto obtenidos en el análisis de riesgos y la clasificación de activos de información de la entidad".*

En este caso, complementando lo anterior, NIST 800-62[30] propone realizar una categorización del impacto del incidente evaluando si se afecta la funcionalidad del sistema de tratamiento, si se afecta la seguridad de la información del tratamiento comprometido y cuál será el esfuerzo para recuperarse del incidente, en este caso en particular, recordemos que se busca priorizar la seguridad de la información, por lo que, esta categoría es la más importante para catalogar el impacto del incidente.

- **Categorías de impacto funcional**

CATEGORÍA	DEFINICIÓN
Ninguno	No causa ningún efecto sobre la capacidad de la institución para proporcionar diversos servicios a todos los usuarios
Bajo	La institución aún puede proporcionar todos los servicios críticos a todos los usuarios, pero ha perdido eficiencia.
Medio	La institución ha perdido la capacidad de proporcionar un servicio crítico a un subconjunto de usuarios del sistema.
Alto	La institución ya no puede proporcionar algunos servicios críticos a ningún usuario

- **Categorías de impacto a la seguridad de la información**

CATEGORÍA	DEFINICIÓN
Ninguno	Ninguna información fue exfiltrada, cambiada, eliminada o comprometida de alguna manera
Violación de privacidad	Se accedió o se exfiltró información que contiene datos personales de las personas titulares.

[29] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Técnologías de la Información y las Comunicaciones de Colombia, última consulta el 31 de octubre de 2024. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[30] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.2.4 Incident Analysis, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Pérdida de información	Se accedió o se exfiltró información que no incluye datos personales de las personas titulares.
Pérdida de integridad	Se cambió o eliminó información que contiene datos personales.

- **Categorías de esfuerzo de recuperabilidad**

CATEGORÍA	DEFINICIÓN
Regular	El tiempo de recuperación es predecible con los recursos existentes
Complementario	El tiempo de recuperación es predecible con recursos adicionales
Extendido	El tiempo de recuperación es impredecible; Se necesitan recursos adicionales y ayuda externa.
No recuperado	No es posible recuperarse del incidente (por ejemplo, datos confidenciales filtrados y publicados públicamente); se debe iniciar una investigación.

Tablas recuperadas de las tablas 3-2, 3-3 y 3-4 de NIST 800-62

B. Clasificación

Una vez definido el impacto, los incidentes a los que nos podemos enfrentar son de manera enunciativa más no limitativa:

i. La pérdida o destrucción no autorizada, es un incidente que involucra la destrucción total o parcial de los activos.
ii. El robo, extravió o copia no autorizada, es un incidente que involucra que los activos de información fueron sustraídos de manera total o parcial.
iii. El uso, acceso o tratamiento no autorizado, Es un incidente que involucra un acceso lógico o físico sin autorización del propietario de un sistema, aplicación, información o un activo de información.
iv. El daño, la alteración o modificación no autorizada, es un incidente que involucra que los activos sufren modificaciones en sus componentes.

C. Priorización

De acuerdo con NIST 800-61[31] los incidentes no deben manejarse por orden de llegada, se deben priorizar en función del impacto por lo que al tener identificado el impacto en las dimensiones de funcionalidad, seguridad de la información y recuperabilidad, se debe relacionar su combinación para dar prioridad en este caso a los incidentes que tienen impacto a la seguridad de la información:

Impacto funcional	Impacto a la seguridad de la información	Impacto a la recuperabilidad
Ninguno	Ninguno	Regular
Bajo	Pérdida de disponibilidad de la información	Complementario
Medio	Pérdida de integridad de la información	Extendido
Alto	Pérdida de confidencialidad de la información	No recuperado

Tabla impacto funcional-a la seguridad de la información-a la recuperabilidad

[31] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.2.4 Incident Analysis, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

D. Definición de tiempo de respuesta

Para el caso de la definición del tiempo de atención de incidentes de seguridad, de acuerdo con la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información[32] del Ministerio de Tecnologías de la Información y Comunicaciones, "*se deben establecer tiempos máximos de atención de los incidentes, con el fin de atender adecuadamente los incidentes de acuerdo a su criticidad e impacto".*

Resaltando que cada entidad es libre de definir tiempos de atención a incidentes como crean conveniente y dependiendo de la criticidad de los activos impactados. Por ejemplo:

Nivel de prioridad	Tiempo sugerido
Bajo	No mayor a dos horas
Medio	No mayor a una hora
Alto	No mayor a 30 minutos
Urgente	De inmediato

Ejemplo de rangos de tiempos por nivel de prioridad

E. Declaración del incidente

Una vez que se está convencido que el evento de seguridad de la información efectivamente es un incidente a la seguridad de la información, la ISO/IEC 27035-1:2016[33] recomienda que una institución debiera realizar las siguientes actividades:

- Recopilar información que pueda incluir pruebas, mediciones, y otros datos obtenidos sobre la detección de un evento de seguridad información. El tipo y cantidad de información recabada dependerá del evento de seguridad de la información que haya ocurrido.
- Realizar una evaluación para determinar si el evento tiene consecuencias de continuidad de negocio o bien sobre afectaciones al derecho de protección de datos personales de los titulares.
- Hay que asegurar que todas las partes involucradas, en particular el equipo de respuesta a incidentes, registran apropiadamente todas las actividades, resultados y las decisiones relacionadas, para su posterior análisis.
- Hay que asegurar de que se realiza un reporte y se realiza la notificación del incidente

4. Contención

Cuando una alerta permite distinguir un incidente de seguridad, se procede a la fase de contención, **a fin de limitar el alcance o impacto del incidente identificado.**

De acuerdo con NIST 800-61[34], "*la contención es importante antes de que el incidente afecte otros recursos o aumente los daños que ha ocasionado, la mayoría de los incidentes requieren contención, por lo que es una consideración importante al principio del manejo de cada incidente".* La contención proporciona tiempo para desarrollar una estrategia de remediación personalizada.

[32] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Técnologías de la Información y las Comunicaciones de Colombia, pp15, última consulta el 31 de octubre de 2024. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
[33] ISO/IEC 27035-1:2016, Principles of incident management, pp 7, última consulta el 31 de octubre de 2024, disponible en: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027035-1-2016.pdf
[34] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.2.4 Incident Analysis, última consulta el 31 de octubre de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Por su parte, la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información[35] del Ministerio de Tecnologías de la Información y Comunicaciones, *"esta fase se busca evitar la difusión del incidente y así reducir los daños a los recursos y componentes tecnológicos, así como reducir la perdida de la confidencialidad, integridad y disponibilidad de la información."*

Para facilitar esta tarea la institución debe poseer una estrategia de contención previamente definida para poder tomar decisiones. *"La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones"*[36]. Algunos criterios que pueden ser tomados como base son:

- Daño potencial
- Preservación de evidencia
- Disponibilidad del servicio
- Tiempo para ejecutar acciones
- Recursos humanos, técnicos y financieros disponibles

La contención no es una erradicación del incidente, pues esta se centra en aislar los activos afectados. Por ejemplo, si se trata de medios de almacenamiento físico, se aísla el entorno donde ocurrió el incidente como el archivero u oficina. O bien, si se trata de un medio de almacenamiento electrónico, se separan los equipos de cómputo afectados de la red, para evitar, por ejemplo, la propagación de una infección de software malicioso.

Se pueden utilizar los formatos de investigación y contención de incidentes del Anexo correspondiente como referencia para el aislamiento de los activos, y posteriormente para la creación de los respaldos (de ser necesaria), y su puesta en operación, a fin de volver a un estado funcional en los sistemas de tratamiento en la entidad.

El aislamiento de sistemas y la puesta en operación de respaldos son acciones a corto plazo para reducir los efectos de un incidente. Para proseguir a la contención del incidente a largo plazo se deben identificar las vulnerabilidades explotadas en los activos, así como las medidas de seguridad que pudieron hacer falta, para su posterior implementación.

5. Mitigación (Erradicación)

De acuerdo con NIST 800-61[37] *"una vez que se ha contenido un incidente, puede ser necesaria la erradicación para eliminar componentes del incidente"*. Para algunos incidentes, la erradicación no es necesaria o se realiza durante la recuperación.

En la recuperación, los administradores restauran los sistemas a su funcionamiento normal, confirman que los sistemas funcionan normalmente y en caso de que corresponda, corrigen las vulnerabilidades para evitar incidentes similares.

La recuperación puede implicar acciones tales como restaurar sistemas a partir de copias de seguridad limpias, reconstruir sistemas desde cero, reemplazar archivos comprometidos con versiones limpias, instalación de parches, cambio de contraseñas y refuerzo de la seguridad del perímetro de la red.

[35] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Técnologías de la Información y las Comunicaciones de Colombia, pp20, última consulta el 11 de febrero de 2024. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
[36] Ibídem pp21
[37] Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, 3.3.4 Erradication and Recovery, última consulta el 11 de febrero de 2024. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Los niveles más altos de registro del sistema o monitoreo de la red suelen ser parte del proceso de recuperación. Una vez que un recurso es atacado con éxito, a menudo se vuelve a atacar o se atacan otros recursos dentro de la institución de manera similar.

La erradicación y la recuperación deben realizarse en etapas para priorizar las medidas de remediación. En el caso de incidentes a gran escala, la recuperación puede llevar meses; La intención de las primeras fases debe ser aumentar la seguridad general con cambios de alto valor relativamente rápidos (de días a semanas) para evitar incidentes futuros.

Las fases posteriores deberían centrarse en cambios a más largo plazo (por ejemplo, cambios de infraestructura) y trabajo continuo para mantener la empresa lo más segura posible.

En resumen, esta etapa involucra la ejecución de un **tratamiento profundo del incidente** de seguridad para minimizar la posibilidad de que éste se repita.

Como se mencionó, esta etapa se considera la creación de un plan de implementación de medidas de seguridad, por ejemplo, para reforzar la seguridad de los medios de almacenamiento físico, se deben mejorar las políticas y los controles de acceso físico, como lo es, mejores cerraduras. Para los medios de almacenamiento electrónico, la mitigación incluye actualizaciones de hardware y software, así como revisiones con herramientas automatizadas sobre los respaldos que se pusieron en operación.

Cuando se cuenta con equipos de respuesta a incidentes avanzados, propios o subcontratados, se inicia el proceso ***de recolección de evidencia para el análisis forense digital***.[38] Es decir, de los activos en medios de almacenamiento electrónicos que se aislaron en la etapa de contención, se realizan ***imágenes forenses*** o copias exactas bit a bit, que se analizan en laboratorios (que pueden ser particulares o de una autoridad de impartición de justicia según corresponda el caso que se investigue), con herramientas especiales de hardware y software, a fin de obtener más información del incidente.

En el Anexo correspondiente se incluye el formato de mitigación, que permite registrar los controles y medidas de seguridad a implementar. Asimismo, se considera el formato de cadena de custodia[39], para continuar con la investigación del incidente que se inició en la fase de contención, a fin de arrojar nueva información para la erradicación y para generar evidencia en caso de continuar con un proceso legal, incluso para la creación de documentos de investigación para aquellos interesados en el tema.

6. Recuperación

En esta etapa se busca desarrollar la capacidad de resiliencia para volver al estado anterior al incidente con los menores daños posibles, por lo que sus actividades se enfocan en dar ***seguimiento a las medidas implementadas en la mitigación, y los activos que fueron afectados se reintegran a los sistemas de tratamiento***, ahora que se encuentran funcionales, o que ya cuentan con medidas de seguridad que los soporten.

La etapa de mitigación considera la creación de dos tipos de planes:

[38] El análisis forense digital es el conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales, y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

[39] El término cadena de custodia alude a la metodología y su documentación, utilizada para dar seguimiento a los indicios de un incidente de seguridad, a fin de evitar su alteración. A través de la cadena de custodia se registran los indicios y todos los involucrados en su manipulación

- **Plan de Continuidad del Negocio**

Documento que da cuenta de la información crítica que necesita una empresa para recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de un incidente no deseado o desastre.

- **Plan de recuperación de desastres**

Documento que contiene instrucciones detalladas sobre cómo responder restaurar el acceso a los sistemas y/o infraestructura comprometida por un incidente de seguridad. El plan contiene estrategias sobre cómo minimizar los efectos de un desastre, para que una institución siga en funcionamiento o pueda recuperarse lo más pronto posible.

No todos los activos afectados pueden volver a la operación normal, en este caso se debe documentar el o los activos que entran en sustitución, y el proceso de eliminación de los activos que ya no serán utilizados.[40]

Esta fase también contempla el monitoreo de los sistemas de tratamiento a fin de identificar si las nuevas medidas de seguridad no causan algún malfuncionamiento en el sistema, o si éstas funcionan adecuadamente. Dependiendo del tamaño o madurez de la institución, el monitoreo podría ser temporal, o permanente a través del uso de herramientas automatizadas.

Se recomienda hacer una simulación del incidente que llevó a la implementación de las medidas de seguridad, para corroborar que dichos controles pueden evitar que un incidente similar se repita. En caso de falla hay que corregir la implementación.

En cuanto se ha comprobado de diversas maneras la erradicación del incidente, se debe realizar el cierre de incidente. Para que, se pueda regresar a la etapa de preparación, a fin de continuar con la implementación de medidas de seguridad que permitan mejorar la atención y detección de alertas, así como la respuesta cuando se presenten nuevos incidentes de seguridad.

En el Anexo correspondiente se incluye el formato de recuperación del incidente para documentar si los activos afectados por un incidente regresaron o no a la operación de rutina y si se mitigaron los riesgos que causaron el incidente.

7. Mejora continua (Aprendizaje) o actividades posteriores al incidente

El propósito de esta fase es **completar la documentación de lo que se hizo respecto al incidente**, y comunicar a las partes interesadas el estado de la seguridad de los activos después del incidente, es decir, la información contenida en esta etapa es necesaria para la preparación continua, donde las lecciones aprendidas se aplican para mejorar la preparación para manejar incidentes futuros.

En esta etapa debe considerar al menos las siguientes actividades:

- Realizar un informe completo y detallado del incidente ocurrido.
- Monitoreo posterior al incidente por si la amenaza reaparece.
- Identificación de medidas preventivas.

[40] Se recomienda revisar la Guía para el Borrado Seguro de Datos Personales, a fin de evitar riesgos con la eliminación de medios de almacenamiento físicos y electrónicos, consultable en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_ Borrado_Seguro_DP.pdf

- Análisis de las lecciones aprendidas.

Las consideraciones importantes para esta fase son las formas en que la identificación podría haber ocurrido antes y la respuesta podría haber sido más rápida o eficaz, las deficiencias organizativas que podrían haber contribuido al incidente y las áreas potenciales de mejora.

Se debe generar un archivo histórico o bitácora que permita a los encargados de la respuesta a incidentes contar con una base de conocimiento, que pueda ser utilizada para entrenar a los usuarios, o a nuevos integrantes del equipo de respuesta a incidentes.

Se recomienda que el reporte final sobre un incidente que se ha erradicado no sobrepase las dos semanas para su elaboración, a fin de no perder detalles importantes sobre lo aprendido.

Si bien, la documentación generada puede utilizarse con fines de entrenamiento general, el reporte completo o la bitácora de incidentes no debería estar a disposición de cualquier usuario, por ello es importante contar con formatos donde se registre a quién se comunica o comparte el aprendizaje de un incidente de seguridad.

En el Anexo I, se incluye un formato de mejora continua como referencia de la estructura del reporte final, así como formatos de comunicación para distribuir el reporte. Si bien, la documentación generada puede utilizarse con fines de entrenamiento general, el reporte completo o la bitácora de incidentes no debería estar a disposición de cualquier usuario, por ello es importante contar con formatos donde se registre a quién se comunica o comparte el aprendizaje de un incidente de seguridad.

Una vez cerrado el incidente, el equipo de respuesta debe regresar a la etapa de preparación, a fin de continuar con la implementación de medidas de seguridad que permitan mejorar la atención y detección de alertas, así como la respuesta cuando se presenten nuevos incidentes de seguridad.

7. Acciones por seguir ante vulneraciones de datos personales

Como se señaló en el apartado 4 de las presentes recomendaciones, los responsables del tratamiento de ambos sectores deben cumplir con ciertas obligaciones tras sufrir un incidente de seguridad que afecta datos personales.

Es así como resulta imprescindible que se desplieguen acciones correctivas inmediatas para tratar, en la medida de lo posible, corregir la situación a fin de que no se materialice el riesgo o bien, mitigar o paliar los efectos de este. Asimismo, para el sector público, es obligatorio elaborar una bitácora, de la que se explica su desarrollo en el apartado correspondiente.

Aunado a lo anterior, los responsables del tratamiento de datos personales tienen la obligación de informar sobre las vulneraciones de seguridad ocurridas, a las personas titulares afectadas[41], a efecto de que puedan tomar las medidas oportunas para la protección de sus derechos morales y patrimoniales.

De conformidad con el artículo 41 de la LGPDPPSO y el artículo 68 de los Lineamientos Generales, dicha notificación debe contener:

1. La naturaleza del incidente; esto es la descripción del entorno y tipo de incidente de que se trata.
2. Los datos personales afectados: implica precisar qué datos fueron comprometidos precisando, por ejemplo, si fueron afectados datos sensibles, sin remitir datos personales dentro de la propia notificación.
3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse. Es decir, un listado de acciones que la persona titular puede realizar para protegerse del impacto del incidente.
4. Las acciones correctivas realizadas de forma inmediata. Se trata de las acciones llevadas a cabo por el responsable para intentar mitigar el impacto del incidente y evitar que se repita, en la medida de lo posible.
5. Los medios donde las personas titulares pueden obtener más información. Esto es establecer un canal de comunicación continua con las personas titulares afectadas.
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente. Esto implica describir de manera sencilla, sin tecnicismos, el incidente, a fin de que las personas titulares comprendan cómo es que se vulneraron sus datos personales.
7. Cualquier otra información y documentación que considere conveniente para apoyar a las personas titulares. Es importante adjuntar información que sea útil para la comprensión del incidente, y para las medidas que puedan tomar las personas titulares para protegerse.

Por otra parte, para el caso de los responsables del sector público, la notificación al INAI o al organismo garante que corresponda es obligatoria[42].

Dicha notificación, debe contener de acuerdo con lo que establece el artículo 67 de los Lineamientos

[41] Artículo 40 de la LGPDPPSO, artículo 68 de los Lineamientos Generales.
[42] Artículo 40 de la LGPDPPSO y artículo 67 de los Lineamientos Generales

Generales:

1. La hora y fecha de la identificación de la vulneración;
2. La hora y fecha del inicio de la investigación sobre la vulneración;
3. La naturaleza del incidente o vulneración ocurrida;
4. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
5. Las categorías y número aproximado de titulares afectados;
6. Los sistemas de tratamiento y datos personales comprometidos;
7. Las acciones correctivas realizadas de forma inmediata;
8. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
9. Las recomendaciones dirigidas al titular;
10. El medio puesto a disposición del titular para que pueda obtener más información al respecto;
11. 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
12. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

La notificación que se realice podrá ser valorada por el Instituto como una medida del cumplimiento por parte del responsable de que está realizando acciones para disminuir los riesgos de una vulneración, sin perjuicio del ejercicio de sus atribuciones de investigación y verificación.

En virtud de lo anterior, en los Anexos 1 y 2 de las presentes recomendaciones, se propone una serie de formatos con los contenidos mínimos establecidos en el marco normativo para la notificación de vulneraciones considerando lo establecido en la LGPDPPSO y en los Lineamientos Generales, mismos que pueden utilizarse a manera de buena práctica por los responsables del sector privado.

Beneficios de la notificación de vulneraciones

Más allá del requerimiento legal, la notificación de vulneraciones debe considerarse como una medida de seguridad que ofrece múltiples beneficios:

1. Puede ayudar a limitar el mal uso de los datos personales, ya que el mismo titular podría tomar acciones para su protección.
2. Permite a los responsables minimizar la pérdida de confianza de las personas titulares, al mostrar que cuando sufren una vulneración de seguridad, toman acciones para mitigar el impacto del incidente.
3. Puede reducir los gastos de mitigación, al evitar la presentación de denuncias, y sus posibles sanciones, por falta de cumplimiento de la obligación legal de notificar la vulneración al titular y, en su caso, a la autoridad.

Proceso de notificación de vulneraciones

La notificación de vulneraciones se debe realizar en el momento adecuado y con la información suficiente, para evitar la exposición de los sistemas de tratamiento y de cualquier otro activo, a fin de que las personas titulares puedan estar protegidos.

A continuación, se presentan las preguntas que un responsable tiene que hacerse para la adecuada notificación de vulneraciones:

¿Cuándo notificar?

En general, se recomienda notificar a las personas titulares (i) en el menor tiempo posible, (ii) cuando ya se tenga información concreta del incidente y (iii) cuando ya no exista exposición de los activos involucrados en la vulneración. Dentro del proceso de respuesta a incidentes, esto ocurre **al final de la etapa de Contención, o bien al inicio de la etapa de Mitigación**.

> **"Dentro de la respuesta a incidentes, el final de la etapa de Contención y el inicio de la etapa de Mitigación son los mejores momentos para notificar una vulneración a la seguridad de los datos personales"**

Los responsables del **sector público** deberán notificar a la persona titular y al INAI las vulneraciones de seguridad dentro de un **plazo máximo de setenta y dos horas**, a partir de que se confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. Dicho plazo comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad[43].

¿Cómo notificar?

El método recomendado de notificación es el **directo** con las personas titulares, es decir por teléfono, correo electrónico, correo postal, o en persona. En caso de que exista urgencia por contactar al titular, puede resultar oportuno utilizar más de un medio de contacto a la vez.

Se puede optar por la notificación indirecta a través de sitios web o medios de comunicación masivos, solamente cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información de contacto.

La **notificación debe ser independiente y personalizada**, y no debe incluir material o información no relacionada con el incidente de seguridad, ya que podría causar confusión.

¿Quién debe notificar?

El **responsable del tratamiento** de los datos personales, incluso si la vulneración ocurrió o involucró a un encargado.

¿A quién se debe notificar además de la persona titular?

Si derivado de la investigación de un incidente se identifica un posible delito, se debe dar parte al Ministerio Público.

Cuando un incidente resulte en una vulneración de seguridad, los responsables del **sector público** tienen la obligación de informar al INAI o al organismo garante de la Entidad Federativa correspondiente, mediante escrito presentado en el domicilio, o bien a través de cualquier otro medio que se habilite para tal efecto.

[43] De acuerdo al Artículo 66 de los Lineamientos Generales.

En algunos casos puede ser conveniente notificar a aseguradoras, instituciones financieras, autoridades de impartición de justicia o a centros de respuesta a incidentes, para obtener asesoría o proporcionar a las personas titulares mayor apoyo.

Para el caso de que un sujeto obligado del orden federal haya sido vulnerado, la notificación debe realizarse al INAI, a través de los siguientes medios:

- **Correo electrónico: investigayverifica@inai.org.mx**
- **Por escrito físico:** entregado en Oficialía de partes en el INAI (Av. Insurgentes Sur 3211, Insurgentes Cuicuilco, alcaldía Coyoacán, C.P. 04530 Ciudad de México, CDMX).

En uno de los anexos se incluye el formato de notificación a personas titulares y para la notificación al INAI o al órgano garante.

8. Lista de revisión para el plan de respuesta a incidentes

A continuación, se presenta una tabla con las preguntas que el equipo de respuesta a incidentes puede tener a la mano (por ejemplo, en la mochila de respuesta a incidentes), además de los formatos de los anexos, para dar seguimiento a un incidente de seguridad:

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Preparación	Identificación de medios de almacenamiento y de medidas de seguridad.	¿Se tienen identificados los medios de almacenamiento físico y electrónico, así como las medidas de seguridad existentes en la institución?	Se debe contar con un inventario de sistemas de tratamiento, medios de almacenamiento y de las medidas de seguridad existentes en la institución.
	Personal designado para la respuesta a incidentes	¿El personal sabe a quién contactar si identifica un incidente de seguridad?	Se debe contar con un directorio o los datos de contacto de la persona o área encargada de atender o dar respuesta a los incidentes.
	Acceso a medios de almacenamiento, medidas de seguridad y herramientas.	¿El personal que puede responder al incidente de seguridad tiene acceso inmediato a los sistemas de tratamiento, los medios de almacenamiento y las medidas de seguridad, inclusive las herramientas que le puedan ayudar con su tarea?	Se debe tener preparada la mochila de respuesta a incidentes.
	Práctica y entrenamiento sobre incidentes de seguridad.	¿El personal ha planteado escenarios de incidentes de seguridad y se ha practicado el cómo responderlos con las medidas de seguridad existentes?	Se deben hacer simulacros tomando como referencia activos y riesgos de la institución. De ser posible, se debe obtener entrenamiento técnico especializado.

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Detección	Ubicación	¿En qué sistema de tratamiento o activos se detectó el incidente?	
	Primer reporte	¿Quién reportó o descubrió el incidente?	
	Descubrimiento de la anomalía	¿Cómo se descubrió el incidente?	
	Reportes adicionales	¿Existen otros reportes que podrían estar relacionados con el incidente descubierto?	
	Alcance del incidente	¿Qué personas (internos y externos), áreas o sistemas de tratamiento están o podrían estar afectados por el incidente de seguridad?	
	Impacto estimado del incidente	¿Cuál es el impacto en las operaciones o procesos de la institución debido al incidente de seguridad?	
	Caracterización del incidente	¿Qué se está haciendo para describir el incidente y documentar las siguientes preguntas sobre éste: ¿qué ocurrió, cuándo comenzó, qué sistemas de tratamiento o procesos afectó, cómo ocurrió?	

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Identificación	Ubicación	¿En qué sistema de tratamiento o activos se detectó el incidente?	
	Primer reporte	¿Quién reportó o descubrió el incidente?	
	Descubrimiento de la anomalía	¿Cómo se descubrió el incidente?	
	Reportes adicionales	¿Existen otros reportes que podrían estar relacionados con el incidente descubierto?	
	Alcance del incidente	¿Qué personas (internos y externos), áreas o sistemas de tratamiento están o podrían estar afectados por el incidente de seguridad?	
	Impacto estimado del incidente	¿Cuál es el impacto en las operaciones o procesos de la institución debido al incidente de seguridad?	
	Caracterización del incidente	¿Qué se está haciendo para describir el incidente y documentar las siguientes preguntas sobre éste: ¿qué ocurrió, cuándo comenzó, qué sistemas de tratamiento o procesos afectó, cómo ocurrió?	

Lista de revisión para responder a un incidente de seguridad			
Etapa	Requisito	Pregunta clave	Notas
Análisis	Evaluación	¿El incidente afecta el derecho a la protección de los datos personales de las personas titulares? ¿Cuál es el impacto del incidente? • Alto • Medio • Bajo	Se debe considerar que el incidente se puede ver en dos sentidos, (i) una afectación al derecho a las personas titulares y (ii) una afectación a la continuidad de operaciones de la institución.
	Clasificación	¿Cuál es el incidente al que se enfrenta? • La pérdida o destrucción no autorizada, es un incidente que involucra la destrucción total o parcial de los activos. • El robo, extravió o copia no autorizada, es un incidente que involucra que los activos de información fueron sustraídos de manera total o parcial. • El uso, acceso o tratamiento no autorizado, Es un incidente que involucra un acceso lógico o físico sin autorización del propietario de un sistema, aplicación, información o un activo de información. • El daño, la alteración o modificación no autorizada, es un incidente que involucra que los activos sufren modificaciones en sus componentes.	Se debe analizar el tipo de vulneración al que se enfrenta.

	Priorización	Tomando como referencia el impacto identificado, ¿Cuál es la criticidad del impacto del incidente? ¿Cuál es el nivel de prioridad de atención a partir de la identificación de los activos comprometidos? • Inmediata • Aplazada	Se debe definir la prioridad de atención del incidente
	Tiempo de respuesta	¿En qué tiempo se pueden recuperar los activos comprometidos? ¿Qué fase se deberá ejecutar considerando el incidente?	Se deben definir tiempos de respuesta
	Declaración	¿Ya cuenta con documentación para declarar el incidente? ¿Está en condiciones de notificar el incidente?	Una vez declarado formalmente el incidente se debe notificar

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Contención	Contención inmediata	¿El incidente representa un problema que se puede aislar de otros procesos en la institución?	En caso afirmativo, proceder a la siguiente pregunta. En caso contrario, identificar cuáles son los elementos mínimos del sistema de tratamiento que se tienen que aislar para mitigar el incidente, con el fin de segregarlos paulatinamente, y proceder a la siguiente pregunta.
	Segregación de activos	¿Se han separado el o los sistemas de tratamiento y los medios de almacenamiento donde se presentó el incidente, de los que no han sido afectados?	En caso afirmativo, continuar con el siguiente requisito. En caso contrario, segregar los componentes del sistema de tratamiento paulatinamente, y proceder al requisito siguiente.
	Generación de imágenes forenses y otra evidencia	Para los sistemas de tratamiento y medios de almacenamiento electrónicos, ¿Se han realizado imágenes forenses de todos los elementos involucrados en el incidente?	Se debe iniciar este proceso si se cuenta con un área o proveedor especializado. En caso de que los activos involucrados en el incidente se relacionen a un delito susceptible de investigación por una autoridad, se debe documentar el acceso o entrega de los mismos para la realización de imágenes forenses.
	Documentación de acciones	¿Se han registrado y documentado todas las acciones que se han realizado desde que se detectó el incidente?	
	Preservación de la documentación y la evidencia	¿La documentación y evidencia de la investigación del incidente se encuentran almacenadas en un lugar seguro?	

	Respaldos y copias de seguridad	¿Se están creando copias de la información de algún activo? ¿Se están utilizando las copias de seguridad y los respaldos existentes para volver a la operación normal antes del incidente?	

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Mitigación (Erradicación)	Plan de implementación de medidas de seguridad	¿Se ha creado un plan de erradicación, con las medidas de seguridad necesarias para que un incidente similar no se repita?	
	Periodo de implementación de medidas de seguridad	¿El plan de tratamiento considera el tiempo en el que se implementarán las nuevas medidas de seguridad?	
	Seguimiento de investigaciones	¿Se está dando seguimiento a las investigaciones que involucraron la generación de imágenes forenses u otra evidencia?	El seguimiento puede consistir tanto en la generación de evidencia para atender un delito, como en conocimiento técnico para conocer más sobre el incidente de seguridad.
Recuperación	Reintegración de los activos	¿Se han actualizado las medidas de seguridad para reintegrar los activos y sistemas de tratamiento afectados por el incidente?	
	Eliminación de activos	¿Se tiene un proceso para la eliminación de los activos que ya no se pueden integrar a los sistemas de tratamiento?	Se deben considerar técnicas de borrado seguro[44]
	Monitoreo de nuevas medidas	¿Se tienen considerados los medios, mecanismos y herramientas para monitorear el desempeño de las nuevas medidas de seguridad?	
	Tiempo de monitoreo	¿Se ha determinado el tiempo de monitoreo o periodo de prueba de las nuevas medidas de seguridad?	
	Pruebas de incidentes	¿Se tiene contemplado realizar pruebas para verificar la efectividad de los controles implementados contra incidentes similares?	

[44] Para mayor referencia se puede consultar la Guía para el Borrado Seguro de Datos Personales, disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

Lista de revisión para responder a un incidente de seguridad			
Etapa	**Requisito**	**Pregunta clave**	**Notas**
Mejora continua: Actividades post incidente (Aprendizaje)	Documentación final del incidente	¿Se tiene ordenada y debidamente almacenada la información generada durante la gestión del incidente?	
	Reporte del incidente	¿Se ha escrito un reporte sobre el incidente, contemplando el qué, cómo, cuándo, y por qué pasó, quienes estuvieron involucrados, el resultado de las investigaciones forenses en su caso, y las medidas de seguridad implementadas o en proceso de implementar?	
	Bitácora de incidente	¿Se ha incluido el reporte dentro de un registro o base de conocimiento con otros incidentes que han ocurrido?	
	Comunicación del incidente	¿Se han realizado las comunicaciones a las partes interesadas de distintas versiones del reporte final?	

Anexo 1. Formato para elaborar una bitácora

FORMATO DE ELABORACIÓN PROPIA

Fecha de elaboración:	

DATOS DE IDENTIFICACIÓN DE QUIEN REPORTA

Datos que detecta el incidente			
Nombre:			
Dirección:			
Teléfono:		**Teléfono móvil:**	
Correo electrónico			

REGISTRO DEL EVENTO

Generales del evento		
Número de evento		
Fecha del evento:		
Hora del evento:		
Cantidad de veces que se repitió el evento:		
Registro del evento:		
Localización del evento:		
Indicador del evento:	[ ] Alerta de seguridad [ ] Reporte de usuario [ ] Anomalía no alertada	
Descripción general del activo o grupo de activos que pudieron haberse comprometido	Nombre del sistema de tratamiento:	
	Tipo de sistema de tratamiento:	
	Responsable del sistema de tratamiento:	
	Personal con acceso al sistema de tratamiento:	
	Tipo de datos involucrados	

	en el evento	
Descripción general precisa de lo ocurrido	¿Qué ocurrió?	
	¿Cómo ocurrió?	
	¿Por qué ocurrió?	
	¿Cuándo ocurrió?	

Clasificación del evento en incidente

Clasificación del incidente:	
Justificación de la clasificación:	
Datos de quien autorizó la clasificación de incidente:	

REGISTRO DEL INCIDENTE
(LLENAR SOLO EN CASO DE CLASIFICAR AL EVENTO COMO INCIDENTE)

Generales del evento	
Descripción del mecanismo de monitoreo que alerto sobre el incidente:	
Medida o medidas de seguridad comprometidas:	
Evaluación del incidente:	
Clasificación del incidente:	[ ] pérdida total de la información [ ] pérdida parcial de la información [ ] destrucción parcial de la información [ ] destrucción total de la información [ ] robo total de la información [ ] robo parcial de la información [ ] extravío parcial de la información [ ] extravío total de la información [ ] generación de copia no autorizada [ ] uso no autorizado [ ] acceso no autorizado [ ] tratamiento no autorizado [ ] daño al activo [ ] alteración del activo [ ] modificación no autorizada [ ] otro: _____-
Prioridad de atención:	
Tiempo programado para la atención del incidente:	
Encargado o encargados de la tarea de recuperación:	

Medidas de seguridad correctivas aplicadas:	
Tipo de daño ocasionado:	
Medidas de seguridad complementarias:	
Descripción de las acciones llevadas a cabo para la mitigación del incidente:	
Descripción de las acciones llevadas a cabo para la recuperación del incidente:	
Observaciones adicionales:	
Nombre del responsable designado:	
Nombre de quien notifica a titulares:	
Nombre de quien notifica al sujeto obligado:	

ANEXO 2. NOTIFICACIÓN DE LA VULNERACIÓN A LOS DATOS PERSONALES

FORMATO PARA EL INAI
FORMATO DE ELABORACIÓN PROPIA

Llenar en caso de que el incidente de seguridad implique una vulneración de datos personales

Fecha de elaboración:	

Descripción del incidente	
Nombre de la institución:	
Hora y fecha de la identificación de la vulneración:	
Hora y fecha del inicio de la investigación sobre la vulneración;	
Naturaleza del incidente:	
Descripción detallada de las circunstancias en torno a la vulneración ocurrida:	
Categorías y número aproximado de titulares afectados:	
Denominación del Tratamiento, Sistema(s) de tratamiento y datos personales comprometidos:	
Acciones correctivas realizadas de forma inmediata:	

Descripción de las posibles consecuencias de la vulneración de seguridad ocurrida:	
Recomendaciones dirigidas al titular:	
Medio puesto a disposición del titular para que pueda obtener más información respecto al incidente:	
Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto:	
Datos de contacto de la o las personas designadas para atender solicitudes respecto al incidente:	

FORMATO PARA NOTIFICAR A LAS PERSONAS TITULARES

FORMATO DE ELABORACIÓN PROPIA

Fecha de elaboración:	

Descripción del incidente	
Nombre de la institución:	
Nombre del sistema de tratamiento:	
Naturaleza del incidente o vulneración ocurrida;	
Datos personales comprometidos;	
Recomendaciones dirigidas al titular sobre las medidas que este pueda adoptar para proteger sus intereses;	
Acciones correctivas realizadas de forma inmediata;	
Medios puestos a disposición del titular para que pueda obtener más información al respecto;	
descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y	
Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.	
Contacto para atender dudas respecto al incidente:	
Observaciones:	

Anexo 3. Recomendaciones a los usuarios contra el software malicioso

Derivado de acontecimientos en materia de seguridad de la información como son las infecciones a nivel mundial a través de las variedades de ransomware[45] #WannaCry[46] y #Petya, el INAI estima pertinente emitir las siguientes recomendaciones para que tanto las instituciones como los usuarios, puedan tomar medidas para su propia protección, a fin de coadyuvar en la minimización del impacto global de los ataques basados en software malicioso.

Los ataques informáticos basados en software malicioso son desarrollados por múltiples partes interesadas, las cuales pueden tener distintos objetivos, como crear redes automatizadas para atacar servicios, extraer o secuestrar información, afectar infraestructura crítica, robar datos de tarjetas de crédito, ganar control de cámaras para obtener imágenes comprometedoras, espiar comunicaciones, entre otras actividades ilícitas.

Por ello, es importante que la ciudadanía en general adopte **una cultura de la ciberseguridad y** tome **medidas de protección contra el *malware***, tales como:

- **Ser cauteloso con los mensajes de desconocidos.** Se debe evitar descargar archivos o dar clic en enlaces, imágenes o contenido proveniente de fuentes desconocidas, sin importar el servicio de mensajería utilizado, por ejemplo, SMS, WhatsApp o bien correo electrónico. Incluso se debe ser cuidadoso cuando un contacto conocido envía información no solicitada, utilizando mensajes de alarma o provocativos.
- **Verificar en lugar de confiar.** Cuando lleguen mensajes relacionados con entidades de gobierno, por ejemplo, la renovación de la visa, el pago de impuestos, o ser apercibido por la policía. O bien, se reciben comunicaciones provenientes aparentemente de servicios, como telefonía o tarjetas de crédito, se recomienda contactar directamente a la entidad o visitar su sitio web y **nunca dar clic a la liga que se proporciona en el mensaje.**
- **Mantener actualizados los dispositivos y utilizar software antivirus.** Todos los dispositivos y equipos de cómputo tienen que estar actualizados, tanto en sus Sistemas Operativos como en sus programas y aplicaciones, esto a fin de disminuir el tiempo de exposición en caso de que exista alguna vulnerabilidad no mitigada por el fabricante. En este sentido, también es importante evitar el uso de software pirata, debido a que este podría no recibir las actualizaciones necesarias para protegerse de malware, o incluso ya estar infectado desde su origen.
- **Realizar respaldos de la información.** Se deben hacer copias de la información crítica de manera periódica. Además, los respaldos deben realizarse ordenadamente y por versiones, es decir no se recomienda sobrescribir la información en cada nuevo respaldo, sino tener al menos las dos últimas versiones de la copia. De manera que, si se tuviera que recuperar información de un dispositivo debido a malware, y también el último respaldo estuviera infectado, se pueda recurrir a la penúltima versión.

[45] El ransomware es un tipo de software malicioso cuyo objetivo es cifrar la información de un equipo de cómputo o dispositivo con la finalidad de secuestrarla, y hacerla inaccesible al dueño a menos que pague un rescate por ella.
[46] México fue el país más afectado en América Latina y el quinto a nivel mundial por el malware #WannaCry, véase: http://eleconomista.com.mx/tecnociencia/2017/05/15/mexico-ya-mas-afectado-wannacry-america-latina

De manera particular, **para que los ciudadanos protejan su información personal contra el acceso de terceros malintencionados**, se pueden tomar medidas como:

- **Usar contraseñas seguras.** Se deben utilizar contraseñas largas y cambiarlas periódicamente, ya que los atacantes utilizan herramientas para buscar y probar contraseñas inseguras en los sistemas y dispositivos.
- **Usar un administrador de contraseñas.** Se puede hacer uso de herramientas de software paraadministrar contraseñas, y así gestionarlas para cada servicio, programa o aplicación que utilice elusuario.
- **Activar la autenticación en dos pasos.** Revisar si un servicio o aplicación tiene algún método para accederlo además de la contraseña, por ejemplo, con un token o un número de confirmación recibidovía celular.
- **Utilizar dispositivos diferentes.** Se recomienda tener equipos de cómputo distintos para cada entorno del usuario, por ejemplo, un celular para el trabajo y otro para asuntos personales, de maneraque en caso de que alguno quede afectado, no exponer toda la información a un atacante.
- **Utilizar conexiones https para navegar por Internet.** Cuando se navega por un sitio de Internet, laspáginas con el prefijo "https" con un candado en verde, protegen la comunicación de punto a punto, es decir un tercero que intercepte la comunicación no podrá ver su contenido. Existen herramientas como HTTPS *Everywhere*[47] de la *Electronic Frontier Foundation* que facilitan esta tarea.
- **Ser cauto con las conexiones WiFi.** Las redes inalámbricas representan un riesgo en virtud de que un atacante puede interceptar las comunicaciones de estas redes, o también crear puntos de acceso falso para que un usuario descuidado se conecte a ellas. Por ello, sólo se deben utilizar puntos deacceso a Internet conocidos y de confianza.
- **Usar servicios de comunicaciones cifradas.** Para comunicaciones de alta importancia no se recomienda utilizar cualquier servicio de mensajería, ya que un tercero podría interceptar la comunicación y acceder a su contenido. Se recomienda utilizar aplicaciones como *Signal*[48], la cualcifra las llamadas y mensajes entre dos usuarios, que para poder comunicarse han tenido queverificar sus claves del servicio por otros medios de contacto, de modo que un tercero que interceptela comunicación no puede acceder al contenido.
- **Cifrar el almacenamiento de los equipos de cómputo.** Las últimas versiones de Windows, Mac OS,iOS y Android tienen funciones para cifrar el almacenamiento local, las cuales se deben activar a fin de no comprometer la información de un equipo de cómputo o dispositivo, en caso de robo, pérdidao extravío.

[47] Véase: https://www.eff.org/es/https-everywhere
[48] Véase: https://signal.org/

Anexo 4. Referencias

Para la elaboración de la presente Guía se tomaron las siguientes referencias nacionales e internacionales:

- CICHONSKI, MILLAR, GRANCE, SCARFONE, Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide, Estados Unidos, National Institute of Standards and Tecnology, 2012. Consultable en: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, última consulta el 31 de octubre de 2024. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- Cómo gestionar una fuga de información. Una guía de aproximación para el empresario, España, Instituto Nacional de Ciberseguridad, 2016. Consultable en: https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion
- Global Guide to Data Breach Notifications, World Law Group, 2016. Consultable en: http://www.theworldlawgroup.com/wlg/global_data_breach_guide_home.asp
- ISO/IEC 27002:2022, última consulta el 31 de octubre de 2024, disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en,
- ISO/IEC 27035:2011 Information technology — Security techniques — Information security incidentmanagement.
- ISO/IEC 27035-1:2016, Principles of incident management, pp 7, última consulta el 31 de octubre de 2024, disponible en: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027035-1-2016.pdf
- ISO/IEC 27000: 2018, última consulta el 31 de octubre de 2024, Versión gratuita descargable en: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- KRAL, WRIGHT, The Incident Handlers Handbook, SANS Institute, 2011. Consultable en: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- SECURITY 504 Hacker Techiniques, Exploits and Incident Handling, Estados Unidos, SANS Institute, 2013.
- Comité Europeo de Protección de Datos (2022). Guidelines 9/2022 on Personal Data Breach Notification under Regulation (EU) 2016/679. Recuperado de: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

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