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

RECOMENDACIONES
para el
Manejo de Incidentes
de Seguridad
de
Datos Personales

Directorio

Francisco Javier Acuña Llamas
Comisionado Presidente

Carlos Alberto Bonnin Erales
Comisionado

Oscar Mauricio Guerra Ford
Comisionado

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Blanca Lilia Ibarra
Comisionada

Joel Salas Suárez
Comisionado

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

Edición • Junio 2018

Contenido

1. Glosario

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

Activos críticos: Activos que un responsable considera como los más valiosos y que, si 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.

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

Disponibilidad:	Propiedad de la información para ser accesible y utilizable cuando se requiera.
Encargado:	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 integridad o la disponibilidad de la información.
Integridad:	Propiedad de la información para salvaguardar la exactitud y completitud de la información.
LFPDPPP:	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LGPDPPSO:	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Lineamientos:	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.
Reglamento de la LFPDPPP:	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Responsable:	En el sector público, 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). En el ámbito privado, es aquella persona física o moral que decide sobre el tratamiento de datos personales (sujeto regulado).

Revelación: Incidente de seguridad en el cual se expone la información a través de Internet o medios masivos de comunicación.

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, 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 63 del Reglamento de la LFPDPPP y 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 organizaciones 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 reguarda el responsable, inclusive, los datos personales, poniendo en riesgo a su titular. Alguno de los incidentes más comunes son los siguientes:

1. Robo de información en documentos y medios de almacenamiento desechados incorrectamente.
2. Empleados que acceden a datos personales sin la autorización correspondiente.
3. Empleados que revelan información a otras personas a través de engaños.
4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal.
5. 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***"

El *2017 Cost of Data Breach Study: Global Overview*[2] señala que **el costo promedio por cada registro** de base de datos perdido o robado con información sensible o confidencial, es de **$141 dólares americanos**. Asimismo, **el promedio mundial de registros expuestos** por cada incidente de seguridad es de **$24,089 dólares americanos**.

Por su parte, el Estudio de la Seguridad de la Información en México 2017[3] señala que **el 87% de las organizaciones mexicanas han tenido incidentes de seguridad de la información** en los últimos doce meses. Adicionalmente, el Estudio de la Privacidad en México 2016[4] indica que el **43% de las empresas mexicanas han sufrido situaciones que implican pérdida, robo o fuga de información**. Sin embargo, sólo el **27% de las organizaciones aseguró contar con procedimientos para la solución de incidentes** operativos en materia de datos personales.

---

[2] Consultable en: https://www.ibm.com/security/data-breach/

[3] Consultable en: https://www.isaca.org/chapters4/Mexico-City/Documents/Estudio%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%20en%20M%C3%A9xico%202017.pdf

[4] Consultable en: http://recursos.pwc.mx/landing.asp?pagina=gracias-por-descargar-estudio-de-la-privacidad-en-mexico-2016

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

Por ello, la normativa de protección de datos personales regula el deber de **seguridad**, el cual señala que todo responsable, tanto del sector público como del privado, que lleve a cabo tratamiento de datos personales tiene la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra vulneraciones.

El Artículo 37 de la LGPDPPSO y el Artículo 63 del Reglamento de la LFPDPPP establecen que las vulneraciones a la seguridad de los datos personales son al menos:

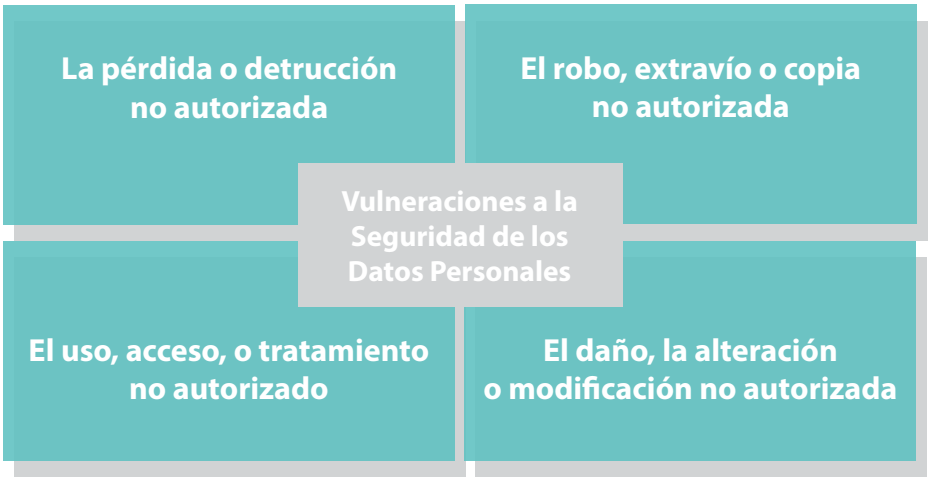

Figura 1. Tipos de vulneraciones a la seguridad de los datos personales

Ahora bien, de acuerdo con el artículo 20 de la LFPDPPP, 63 a 66 de su Reglamento, así como los artículos 36 a 41 de la LGPDPPSO, los responsables del tratamiento están obligados a notificar las vulneraciones que ocurran en cualquier fase del tratamiento de datos, que afecten de forma significativa los derechos patrimoniales o morales de los titulares[5], así como tomar medidas preventivas, correctivas y de mejora para evitar nuevas vulneraciones.

De manera adicional, los responsables de la LGPDPPSO deben notificar las vulneraciones al Instituto o a los organismos garantes, según corresponda.

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

[5] De acuerdo al Artículo 66 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, finanzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular. Se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

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. Plan de respuesta a 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, **en 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.

Para ello se desarrollará (i) la relación entre las alertas y los incidentes de seguridad, (ii) las características particulares de un incidente de seguridad cuando involucra datos personales y; (iii) las etapas del plan de respuesta a incidentes de seguridad.

4.1 Alertas e incidentes de seguridad

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, riesgo, alerta, incidente, vulneración y revelación**.

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

Estos activos son susceptibles a amenazas, es decir, a factores externos que tienen el potencial de dañarlos, 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 2). **Cuando un riesgo se materializa, ocurre un incidente de seguridad**, el cual se traduce en una violación a las **medidas de seguridad**.

Figura 2. Estructura de un riesgo

> "Un incidente de seguridad es un riesgo materializado"

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.

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.

[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, en la sección de Seguridad de los Datos Personales del sitio web del INAI en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

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.

Tabla 1. Ejemplos de alertas de seguridad

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 masivos de comunicación, y
j) Sitios web especializados.

Por ejemplo, derivado de la queja de un titular, un responsable podría enterarse que los datos personales de sus clientes se están utilizando por un tercero no autorizado. O bien, que una organización se entere de que sus sistemas de tratamiento han sido comprometidos o hackeados, a través de una publicación en medios masivos de comunicación.

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, etc.
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[7]	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. 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 masivos de comunicación de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas.

Tabla 2. Ejemplos de incidentes de seguridad

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:

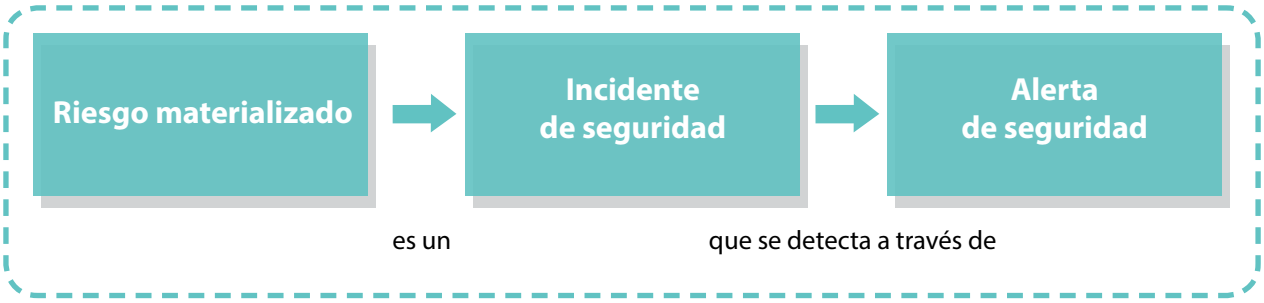

Figura 3. Relación entre riesgos, incidentes y alertas de seguridad.

[7] En el Anexo 2 de este documento se desarrolla una serie de recomendaciones para que los usuarios se protejan contra el software malicioso, más allá de las premisas de la organización, y así minimizar incidentes de seguridad en los sistemas de tratamiento.

4.2 Incidentes de seguridad que afectan datos personales

Por su parte, **las vulneraciones a la seguridad de los datos personales o vulneraciones de seguridad**, mencionadas en los artículos 20 de la LFPDPPP y 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 los titulares de los datos personales.

A su vez, derivado de una vulneración de seguridad, los responsables tienen el deber de analizar las causas por las cuales se presentó ésta, e implementar **las medidas de seguridad preventivas y correctivas para evitar que incidentes similares se repitan**[8].

Para el **sector privado**, estos incidentes implican, además:

a) Informar a los titulares de los datos personales lo siguiente[9]:

   1. La naturaleza del incidente.
   2. Los datos personales afectados.
   3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
   4. Las acciones correctivas realizadas de forma inmediata.
   5. Los medios donde los titulares pueden obtener más información.

b) La imposición de sanciones[10] por parte del INAI, las cuales podrán atenuarse[11] en caso de que el responsable haya atendido las Recomendaciones en materia de seguridad de datos personales del Instituto, publicadas en el Diario Oficial de la Federación.[12]

Por su parte, para el **sector público**, estos incidentes consideran:

a) Informar a los titulares de los datos personales lo siguiente[13]:

   1. La naturaleza del incidente.
   2. Los datos personales afectados.
   3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.

---

8 De acuerdo al Artículo 66 del Reglamento de la LFPDPPP y al Artículo 37 de la LGPDPPSO.

9 De acuerdo al Artículo 65 del Reglamento de la LFPDPPP.

10 De acuerdo al Artículo 63, Fracción XI de la LFPDPPP.

11 Según lo señalado en el Artículo58 del Reglamento de la LFPDPPP.

12 Consultables en: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

13 De acuerdo al Artículo 41 de la LGPDPPSO y al Artículo 68 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde los titulares pueden obtener más información.
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.
7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

b) Informar al INAI o al organismo garante de la Entidad Federativa correspondiente de la vulneración de seguridad ocurrida.

c) La actualización del documento de seguridad correspondiente.

d) Contar con una bitácora de las vulneraciones[14] en la que se describa:

1. En qué consistió la vulneración.
2. La fecha en la que ocurrió.
3. El motivo o causa de la vulneración.
4. Las acciones correctivas implementadas de forma inmediata y a largo plazo.

e) La imposición de sanciones por la autoridad correspondiente debido a la falta de implementación de medidas de seguridad.

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

Finalmente, las **revelaciones** son incidentes de seguridad **que exponen la información a través de Internet o en medios masivos de comunicación**. Las revelaciones de información pueden resultar en una vulneración de seguridad al exponer datos personales a un sin número de terceros.

Cuando se identifica que una revelación expone datos personales, el responsable debe tomar todas las medidas que estén a su alcance para mitigar la difusión o publicación de los mismos. 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 los titulares.

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:

[14] De acuerdo al Artículo 39 de la LGPDPPSO.

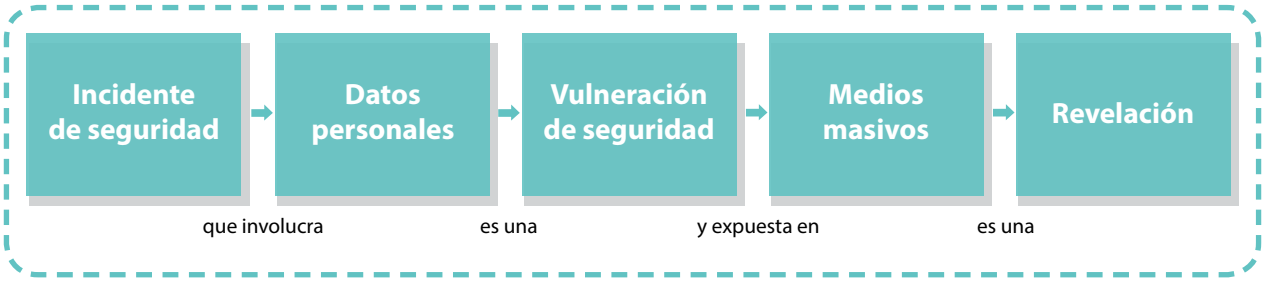

Figura 4. Incidentes de seguridad que comprometen datos personales

4.3. Etapas del plan de respuesta a incidentes de seguridad

A continuación, se desarrollan las **seis etapas** mínimas 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.

A. Preparación

A.1. Consideraciones generales

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"

En el mejor escenario, se recomienda el desarrollo de un Sistema de Gestión de Seguridad de Datos Personales,[15] a fin de identificar los activos en los sistemas de tratamiento, así como los riesgos y medidas de seguridad existentes.

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 tienen que identificar los siguientes elementos que servirán como base del plan de respuesta, en caso de que se presente un incidente de seguridad, a saber:

1. Los activos que son relevantes para la organización.
2. Las medidas de seguridad que tienen los activos.
3. Las alertas de seguridad, asociadas con dichas medidas o controles.
4. Los propósitos de las medidas de seguridad para mitigar un incidente.

[15] Se puede consultar la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales, en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Por ejemplo, para una organización 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 los 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.

Tabla 3. Inventario de preparación ante incidentes.

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 organización.

A.2. Respaldos o copias de seguridad

La creación de respaldos o copias de seguridad es una medida particularmente importante, ya que permite a las organizaciones **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 organización, 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:

- **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.
- **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.
- **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.

A.3. Elementos para la respuesta a incidentes

Cuando el tamaño de la organización 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 1** 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 organización, 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 anterior, 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 1 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 el jefe 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 **5. Lista de revisión para la respuesta a incidentes**, y algunas listas específicas con comandos a ejecutar para sistemas operativos y herramientas.[16]

[16] 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

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 qué, 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 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[17].
  - 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 organización, más que la estrictamente necesaria para su propio uso.

Bajo 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.

[17] 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.

Entrenamiento: Las organizaciones 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"

B. Identificación

En esta etapa **se detectan las alertas de seguridad y se determina si éstas son incidentes**.

Un solo evento no siempre es un indicador de un incidente, por ello se tienen que revisar si hay otras notificaciones o alertas, o bien el equipo de respuesta a incidentes debe buscar otros indicadores que den muestra de que los activos han sido afectados. Entre más información se pueda recabar, existirá mayor certeza respecto a la naturaleza del incidente.

Existen alertas de seguridad cuya naturaleza refleja 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, sin embargo, 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 1** para documentar una o más alertas que se consideren relevantes o que se relacionen con un incidente de seguridad.

Se recomienda 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.

C. 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**.

Durante la contención se tienen que 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 1** 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 organización.

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.

D. Mitigación (Erradicación)

En esta etapa se realiza el **tratamiento profundo del incidente** de seguridad para minimizar la posibilidad de que éste se vuelva a repetir.

La etapa de mitigación 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, por ejemplo, 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***.[18] 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 (privados 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 1** 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[19], 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.

E. Recuperación

En esta etapa se da **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.

[18] 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.

[19] 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.

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.[20]

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 organización, 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 vuelva a repetir. En caso de falla hay que corregir la implementación.

En el **Anexo 1** 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.

F. Mejora continua (Aprendizaje)

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.

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.

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.

[20] 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

5. Notificación de vulneraciones a la seguridad de los datos personales

La notificación de vulneraciones de seguridad es un requisito contemplado en la normativa mexicana en materia de protección de datos personales, para que los titulares puedan tomar medidas para la protección de sus derechos morales y patrimoniales.

En el caso del sector público, la notificación al INAI o al organismo garante que corresponda, también es obligatorio.

En esta sección se desarrollarán algunas consideraciones que permitan a los responsables atender este deber adecuadamente.

5.1 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:

- Puede ayudar a limitar el mal uso de los datos personales, ya que el mismo titular podría tomar acciones para su protección.
- Permite a los responsables minimizar la pérdida de confianza de los titulares, al mostrar que cuando sufren una vulneración de seguridad, toman acciones para mitigar el impacto del incidente.
- 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.

5.2 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 los titulares puedan estar protegidos.

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

1) ¿Cuándo notificar?

En general, se recomienda notificar a los 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 al 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[21].

2) ¿Cómo notificar?

El método recomendado de notificación es el **directo** con los 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.

3) ¿Quién debe notificar?

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

4) ¿A quién se debe notificar además del 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, al menos lo siguiente:[22]

[21] De acuerdo al Artículo 66 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

[22] De acuerdo al Artículo 67 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

a) La hora y fecha en que se identificó la vulneración;

b) La hora y fecha en que inició la investigación sobre la vulneración;

c) La naturaleza de la vulneración ocurrida;

d) La descripción detallada de cómo ocurrió la vulneración;

e) Los tipos de datos personales comprometidos y el número aproximado de titulares afectados;

f) Los sistemas de tratamiento comprometidos;

g) Las acciones correctivas realizadas de forma inmediata;

h) La descripción de las posibles consecuencias de la vulneración ocurrida;

i) Las recomendaciones dirigidas al titular;

j) El medio puesto a disposición del titular para que obtenga mayor información sobre la vulneración y cómo proteger sus datos personales;

k) El nombre completo de la o las personas designadas para proporcionar mayor información al INAI o al órgano garante correspondiente, en caso de requerirse, y;

l) Cualquier otra información o documentación que considere conveniente hacer del conocimiento del INAI o del órgano garante correspondiente.

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 los titulares mayor apoyo.

5) ¿Qué se debe notificar a los titulares?

El contenido de una notificación a los titulares puede variar dependiendo de la vulneración ocurrida. Sin embargo, la información que proporcione el responsable debe servir para que el titular entienda el incidente y pueda prevenir una mayor afectación, la notificación debe considerar al menos:

a) **Descripción de la vulneración:** Se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, así como el periodo en el que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

b) **Datos personales involucrados:** Una descripción de la información involucrada en el incidente.

c) **Recomendaciones a los titulares:** El listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.

d) **Acciones correctivas o de mitigación:** Una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.

e) **Información de contacto:** Datos de las áreas designadas, mesas de servicio o del personal de la organización que puede atender dudas y proporcionar información adicional del incidente.

f) **Fuentes de información adicional:** Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad, en su caso.

6. 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 del **Anexo 1**, 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 organización?	Se debe contar con un inventario de sistemas de tratamiento, medios de almacenamiento y de las medidas de seguridad existentes en la organización.
	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 organización. De ser posible, se debe obtener entrenamiento técnico especializado.

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 organización 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**
Contención	Contención inmediata	¿El incidente representa un problema que se puede aislar de otros procesos en la organización?	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[23].
	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?	

[23] 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 (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?	

Tabla 4. Lista de revisión para responder a un incidente de seguridad.

Anexo 1.
Formatos de referencia para documentar la respuesta a un incidente de seguridad

En este anexo se incluye una serie de formatos que pueden utilizarse por los responsables como referencia para documentar y atender los incidentes de seguridad en sus organizaciones.[24] Por lo tanto pueden adaptarlos y modificarlos a sus necesidades específicas.

Cuando, derivado del seguimiento de un incidente de seguridad, se deban recabar datos personales, el responsable deberá presentar el aviso de privacidad correspondiente.[25]

A. Preparación

A.1 Formato de lista de contactos. Tiene la finalidad de crear un directorio de las personas o áreas clave con las que se debe mantener comunicación directa en caso de un incidente de seguridad.

B. Identificación

B.1 Formato de identificación del incidente. Se utiliza para dar seguimiento al incidente, desde el usuario que reporta hasta el área que atiende la alerta.

C. Contención

C.1 Formato de investigación del incidente. Sirve para documentar el estado del sistema de tratamiento donde ocurrió el incidente.

C.2 Formato de contención del incidente. Se utiliza para documentar el aislamiento parcial o total de un sistema, y realizar los respaldos necesarios si aún se cuenta con ellos.

D. Mitigación (Erradicación)

D.1 Formato de mitigación del incidente. Sirve para documentar las acciones a corto y mediano plazo después de la contención y el respaldo de la información.

D.2 Formato de cadena de custodia. Es un tipo de formato especial cuando además de la respuesta al incidente, se continúa con investigaciones de mayor profundidad en el sistema de tratamiento.

---

[24] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

[25] Para saber más sobre la elaboración de avisos de privacidad, se puede consultar el ABC del aviso de privacidad, consultable en: http://abcavisosprivacidad.ifai.org.mx/

E. Recuperación

E.1 Formato de recuperación del incidente. Se utiliza para documentar la vuelta a las operaciones normales en el sistema de tratamiento.

F. Mejora continua (Aprendizaje)

F.1 Formato de mejora continua. Se utiliza para compartir el conocimiento generado durante el incidente con la organización.

A.1 Formato de lista de contactos[26]

CONTACTOS INTERNOS

Responsable de Datos Personales/Privacidad					
Estructura más alta de funciones relativas a la protección de los datos personales y privacidad de una entidad.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Equipo de Respuesta a Incidentes					
Expertos en materia de respuestas a incidentes de seguridad y protección de datos personales.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Asuntos Jurídicos					
Experto en materia legal, con especialización en materia de datos personales, responsable de dar atención, repuesta y seguimiento a los asuntos jurídicos de la entidad, garantiza que las acciones y procedimientos de respuesta a incidentes cumplen con los requerimientos legales y regulatorios.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Tecnologías de Información					
Responsable del desarrollo, implementación y operación de la política de tecnologías de la información de una entidad, experto en materia de servicios de TI.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Seguridad de la Información					
Responsable de la seguridad de la información de la entidad, contribuye en la atención de los incidentes de seguridad y protección de datos personales.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

[26] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

Administrador de Incidentes					
Miembro del equipo de respuesta a incidentes, lleva a cabo tareas de respuesta a incidentes para contener la exposición derivada de un incidente, documenta las acciones realizadas, mantiene la cadena de custodia y apoya en la redacción del informe y las lecciones aprendidas.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Investigador					
Especialista que realiza tareas de investigación, sobre un incidente específico, determina el origen de la causa, redacta informes sobre sus hallazgos.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Especialista de Seguridad de TI					
Experto en materia de tecnologías de información y seguridad, miembro del equipo de respuesta a incidentes, realiza tareas complejas y exhaustivas relativas a la seguridad de TI, realiza evaluación/auditoría de seguridad de TI como medida proactiva.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Área/Negocio					
Responsable de la operación del área o negocio, dueño de los activos/sistema de información.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Recursos Humanos					
Experto en el área de recursos humanos, proporciona asistencia en la gestión/respuesta a incidentes cuando sea necesario realizar una investigación a un empleado involucrado en el incidente, para proteger la marca y la reputación de la organización.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Relaciones Públicas					
Experto en relaciones públicas que apoyará a realizar una comunicación controlada a las partes interesadas tanto internas como externas para reducir cualquier impacto adverso en las actividades de respuesta a incidentes en curso.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Especialista en Gestión de Riesgos					
Experto en materia de gestión de riesgos que trabaja de forma cercana con el responsable del área/negocio, para determinar y manejar el riesgo.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Responsable de Seguridad Física e Instalaciones					
Responsable de las instalaciones físicas de la entidad, responsable de asegurar la seguridad física durante los incidentes.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro					
Especificar					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

CONTACTOS EXTERNOS

Soporte Técnico del Proveedor de Servicios de Internet					
Área de soporte del proveedor de conectividad (Internet) que brinda atención técnica.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Autoridad en Materia de Protección de Datos Personales					
INAI					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Empresa/ Institución/ Autoridad					
Especificar:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Autoridad Local Facultado para Atender Delitos Electrónicos					
Autoridad local que investiga, da seguimiento y sanciona delitos que hacen uso de tecnologías de la información para vulnerar la información o datos personales.					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

OTROS CONTACTOS

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Otro (especificar)					
Descripción:					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

B.1 Formato de identificación de incidentes[27]

INFORMACIÓN GENERAL
(para ser llenado por quien detecta el incidente)

Información del personal que detecta el incidente					
Nombre:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

Información sobre el incidente				
Fecha:		Hora:		
Localización donde se detectó el incidente:				

Tipo de sistema de tratamiento: ☐ Físico ☐ Electrónico

Nombre del responsable del sistema de tratamiento:

Se encuentran involucrados datos personales en el incidente: ☐ Sí ☐ No

Tipo de datos personales involucrados:

Descripción de lo sucedido:

Evaluación (para ser llenado por el equipo de gestión de incidentes)

Una vez analizada la información, se determina que se trata de un incidente de seguridad: ☐ Sí ☐ No

Justificación:

Mencionar si existe algún posible impacto legal o contractual por el incidente:

[27] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

RESUMEN DEL INCIDENTE (para ser llenado por el equipo de gestión de incidentes)

RESUMEN EJECUTIVO DEL INCIDENTE

RESUMEN TÉCNICO DEL INCIDENTE					
Tipo de Incidente	☐ Denegación de servicio	☐ Uso no autorizado	☐ Espionaje		
	☐ Código malicioso	☐ Acceso no autorizado	☐ Robo, pérdida o extravío		
	☐ Ingeniería social	☐ Otro: _____			

Sitio/Área/ Departamento donde se presentó el incidente:					
Nombre del contacto en el sitio donde se presentó el incidente:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			
¿Cómo fue detectado el incidente?					
Información adicional					
Firma					
Nombre y firma del personal que detecta el incidente			Nombre y firma del personal representante del Equipo de Gestión de Incidentes		

C.1 Formato de investigación del incidente[28]

DATOS PARA INVESTIGACIÓN			
Ubicación de los sistemas de tratamiento afectados			
Sistema afectado:		Sitio:	

Tiempos			
Fecha y hora en que se detectó el incidente		Fecha y hora en que los especialistas en incidentes llegaron al sitio	
Fecha:		Fecha:	
Hora:		Hora:	

Descripción			
Sistema de tratamiento afectado:			
¿El sistema de tratamiento afectado es físico o electrónico?	☐ Físico	☐ Electrónico	

SISTEMAS DE TRATAMIENTO FÍSICO	
Sistema de tratamiento	
Describa los controles de seguridad físicos que identifique de la inspección ocular	
Personas que tienen acceso al sistema de tratamiento	
SISTEMAS DE TRATAMIENTO ELECTRÓNICO	
Sistema de tratamiento	
Describa los controles de seguridad físicos que identifique de la inspección ocular	

¿El sistema afectado está conectado a una red?	☐ Sí	☐ No

Dirección de red del sistema		Dirección MAC	

¿El sistema afectado está conectado a un punto de acceso a Internet?	☐ Sí	☐ No
Número de teléfono:		

¿Se contrataron los servicios de personal externo para apoyar o realizar la gestión del incidente?
Sí / No Describir las acciones realizadas por el personal externo para la gestión o apoyo del incidente.

[28] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

C.2 Formato de investigación del incidente[29]

ACCIONES DE CONTENCIÓN				
1. Aislamiento de los sistemas de tratamiento afectados:				
¿El Comité de Respuesta a Incidentes aprobó el aislamiento / bloqueo / resguardo?		☐ Sí	☐ No	
Acción aprobada:	☐ Aislamiento	☐ Bloqueo	☐ Resguardo	☐ Reubicación
Sí			No	
Hora:		Fecha:	Describir la razón de la negativa	
2. Respaldo de los sistemas afectados:				
¿Se cuenta con respaldo del sistema de tratamiento afectado?		☐ Sí	☐ No	
Si no se cuenta con respaldos, ¿es necesario respaldar?		☐ Sí	☐ No	
Si se realizó un respaldo, ¿fué exitoso para todos los sistemas?		☐ Sí	☐ No	
Acciones realizadas para hacer el respaldo:				
Nombres de las personas que realizaron el respaldo:				
Fecha de inicio del respaldo:		Fecha de término del respaldo:		
Hora de inicio del respaldo:		Hora de término del respaldo:		
Mecanismo empleado para el respaldo				
Físicos				
☐ Copias fotostáticas	☐ Sitio alterno	☐ Otro:		
Electrónicos				
☐ Cintas	☐ CD/DVD/ USB	☐ Digitalización		
☐ Disco duro	☐ Nube	☐ Otro:		
¿El mecanismo de respaldo fue sellado?	☐ Sí	☐ No		
Fecha del sello:		Hora del sello:		
Nombre de la persona a quién fue entregado el respaldo o es responsable de su resguardo:				
Sitio donde se almacenó el respaldo:				
¿Se realizaron pruebas al respaldo?	☐ Sí	☐ No		
Mecanismos utilizados para las pruebas				
Nombre y firma de quién realiza el respaldo		Nombre y firma de quién recibe y valida el respaldo		

[29] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

D.1 Formato de mitigación del incidente[30]

DESCRIPCIÓN DE LAS ACCIONES DE MITIGACIÓN		
1. Personal involucrado		
Nombre de las personas que realizaron el análisis del sistema de tratamiento afectado:		
Iniciales	Nombre completo	Puesto

2. Descripción de las vulnerabilidades detectadas:			
¿Fueron identificadas vulnerabilidades?	☐ Sí	☐ No	
Tipo de activo[31]	Vulnerabilidad	Descripción	Impacto
			Alto
			Medio
			Bajo
Acciones realizadas para erradicar las vulnerabilidades detectadas			

3. Validación:
¿Cuál fue el procedimiento de validación usado para asegurar que el problema fue erradicado?

4. Cierre:	
Fecha y hora del cierre del incidente:	
Nombre y firma de quién realiza la erradicación	Nombre y firma de quién validó la erradicación

[30] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

[31] Véase el apartado "Anexo A. Ejemplos de Activos" de la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, consultable en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

D.2 Formato de investigación del incidente[32]

Procesamiento de indicios o evidencias		
1. Identificación de los indicios o evidencias:		
Número de indicio o evidencia	Descripción del indicio o evidencia	Estado en que se encontraba
1	Si es un dispositivo físico, incluir modelo y número de serie	
2		

2. Fijación de los indicios o evidencias:				
Fotográfica:	Sí ☐	No ☐		
Videograbación:	Sí ☐	No ☐		
Por escrito:	Sí ☐	No ☐		
Otros:				
Observaciones				

3. Recolección o levantamiento:
a) Descripción de la forma en que se realizó:
b) Medidas tomadas para preservar la integridad del indicio o evidencia:

4. Entrega de indicios o evidencias					
Fecha:			Hora:		
Nombre de la persona que entrega:					
Cargo de la persona que entrega:					
Tipo de indicio o evidencia					
Tipo de embalaje y condiciones en que se entrega el embalaje					
Documentos					
Observaciones al estado en que se reciben los indicios o evidencias					
Nombre y firma de quién entrega			Nombre y firma de quién recibe		

[32] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

E.1 Formato de recuperación del incidente[33]

DESCRIPCIÓN DE LAS ACCIONES DE RECUPERACIÓN		
1. Continuidad en la operación		
El sistema de tratamiento continua con su operación después del incidente:	☐ Sí	☐ No
En caso de "No" indicar las causas:		
PERSONAL DESIGNADO PARA DAR SEGUIMIENTO A LA RECUPERACIÓN DEL INCIDENTE		
Iniciales	Nombre completo	Puesto

2. Tiempos:		
Fecha en que fue detectado	Fecha en que fue atendido por el equipo de respuesta a incidentes	Fecha en que fue cerrado
Hora en que fue detectado	Hora en que fue atendido por el equipo de respuesta a incidentes	Hora en que fue cerrado

3. Monitoreo:	
Describir las acciones que se realizarán para monitorizar las medidas implementadas:	
Describir las herramientas para el monitoreo de las medidas implementadas (si es el caso):	
Nombre y firma de quién realiza la recuperación	Nombre y firma de quién validó la recuperación

[33] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

F.1 Formato de recuperación del incidente[34]

DOCUMENTACIÓN DEL INCIDENTE	
1. Descripción:	
Área involucrada:	
Sistema de tratamiento afectado:	
Información/ datos personales involucrados en el incidente:	
Resumen Ejecutivo	
Acciones realizadas	
Impacto a la organización / institución	

REGISTROS DE COMUNICACIÓN SOBRE EL INCIDENTE					
Comunicación entre A-B					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

[34] Estos formatos son una adaptación de los puestos a disposición por el Instituto SANS en su sitio web, consultables en: https://www.sans.org/score/incident-forms

Comunicación entre B-C					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Comunicación entre C-D					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Anexo 2.
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[35] #WannaCry[36] y #Petya, el INAI estima pertinente emitir las siguientes recomendaciones para que tanto las organizaciones 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.

[35] 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.

[36] 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 para administrar contraseñas, y así gestionarlas para cada servicio, programa o aplicación que utilice el usuario.
- **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 recibido vía 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 manera que 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, las páginas 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*[37] 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 de acceso 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*[38], la cual cifra las llamadas y mensajes entre dos usuarios, que para poder comunicarse han tenido que verificar sus claves del servicio por otros medios de contacto, de modo que un tercero que intercepte la 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, pérdida o extravío.

[37] Véase: https://www.eff.org/es/https-everywhere

[38] Véase: https://signal.org/

Anexo 3.
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
- 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 27035:2011 Information technology — Security techniques — Information security incident management.
- 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.

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