TOOLKIT DE CONCIENTIZACIÓN DE SEGURIDAD DE DATOS PERSONALES PARA RESPONSABLES DEL SECTOR PRIVADO

MÓDULO 2. Amenazas

Índice

Conceptos

- **Activos:** Es cualquier valor para la organización que requiera ser protegido. En el caso de la seguridad de los datos personales, deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Los activos se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo. [1]

Ejemplos:

- **Activos de información**, corresponden a la esencia de la organización:
  - Información relativa a los datos personales.
  - Información de procesos del negocio en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de estos.
- **Activos de apoyo**, en los cuales residen los activos de información:
  - Hardware (ej. computadora).
  - Software (ej. procesador de textos.)
  - Redes y telecomunicaciones (ej. Internet).
  - Personal.
  - Estructura organizacional.
  - Infraestructura adicional.

Los activos se pueden clasificar de la siguiente manera:

- Información.
- Conocimiento de procesos del negocio.
- Hardware (consiste en todos los elementos físicos que soportan procesos de datos personales).
- Soportes (medios de almacenamiento de datos personales).
- Software (consiste en todos los programas y aplicaciones que contribuyen a al procesamiento de datos personales).

[1] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf.

- Redes y telecomunicaciones (consisten en todos los dispositivos usados para interconectar computadoras o elementos de un sistema de información de voz y/o datos.
- Sitio (comprende todos los lugares o locaciones que contienen a los activos y procesos, así como los medios físicos necesarios para operar).
- Personal y organización (consiste en todas las personas involucradas en la operación del Sistema de Gestión de Datos Personales, así como sus funciones, roles o procedimientos asignados).

- **Amenaza:** Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo la misión, las funciones, la imagen o la reputación), los activos de la organización o los individuos a través de un sistema de información mediante el acceso no autorizado, la destrucción, la divulgación, la modificación de la información y/o la denegación de servicio. También, el potencial de una fuente de amenaza para explotar con éxito una vulnerabilidad particular del sistema de información.[2]

Ejemplos:
- Incendio.
- Robo de documentos y equipo.
- Alteración de software y hardware.
- Fallas en el equipo.
- Uso no autorizado del equipo.

- **Ciclo de vida de los datos personales**: Las actividades consideradas dentro del ciclo de vida de los datos personales son obtención, almacenamiento, uso, divulgación, bloqueo y cancelación. La obtención de datos personales comprende todas las tareas en donde los datos personales son creados de manera directa por fuentes autorizadas o en forma indirecta a través de transferencias o generados mediante procedimientos de deducción. El almacenamiento es el proceso por medio del cual se guardan los datos personales en forma electrónica,

[2] Disponible en: https://csrc.nist.gov/glossary/term/threat.

impresa o cualquier otro medio. El uso de los datos personales implica el acceso, manejo y procesamiento para el propósito que fueron creados. La divulgación consiste en las remisiones y transferencias de los datos personales hacia otras instancias que requieren y tienen autorización para el tratamiento de los datos personales. El bloqueo se realiza cuando los datos personales ya no son de utilidad, pero por alguna disposición regulatoria interna o externa deben retenerse. La cancelación o destrucción de datos personales implica la eliminación de la información cuando deja de ser útil para el propósito que fue creada.[3]

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

- **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.[4]

- **Vulneración de seguridad:** Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento y que ocasiona 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.[5]

- **Ingeniería social:** Es una técnica utilizada para obtener información de las personas teniendo como base la interacción social, la manipulación y el engaño, y ocurre típicamente en conversaciones directas entre el delincuente y la víctima. El estafador consigue que su víctima no se dé cuenta cómo ni cuándo dio todos los datos necesarios para el robo de su identidad. En esta práctica se recurre a la manipulación de la

[3] Disponible en: https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProteccionDatosPersonales.pdf.
[4] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf.
[5] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf.

psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que, en la cadena de seguridad de la información, el ser humano es el eslabón más débil: la propia víctima es la que otorga su información.[6]

Ejemplos:

- **Pretexting:** Es una variación de la ingeniería social, con la diferencia de que, para realizarla, el atacante debe tener un estudio previo de la información de la víctima potencial, para así, crear y utilizar un escenario favorable con el objetivo de persuadir a una víctima y obtener información. El atacante puede acoplarse a una víctima específica de manera que aumenta la posibilidad de conseguir información o que la víctima realice acciones específicas a su voluntad.
- **Extorsión telefónica:** Es una variación de la ingeniería social, en la cual el atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, por ejemplo, un técnico de soporte o un empleado de alguna organización con el objetivo de obtener datos de la víctima, de un modo muy efectivo, lo único que se requiere es un teléfono.

- **Terrorista informático:** Persona que recurre al uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno (ciberterrorismo o terrorismo electrónico).[7]

- **Hacktivista:** Un hacktivista utiliza las mismas herramientas y técnicas de un hacker, pero lo hace con el fin de interrumpir los servicios y brindar atención a una causa política o social.[8]

- **Cracker:** Los crackers o hackers de sombrero negro son esas personas que usan todo su talento y conocimiento no para el bien sino para romper sistemas informáticos o entrar de forma

[6] Disponible en: https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Gu%C3%ADa_Prevenir_RI.pdf.
[7] Disponible en: https://www.corteidh.or.cr/sitios/tesauro/tr2652.htm.
[8] Disponible: https://www.ecured.cu/Hacktivistas.

ilícita en sistemas informáticos; esto es un delito y eso hay que tenerlo muy claro.[9]

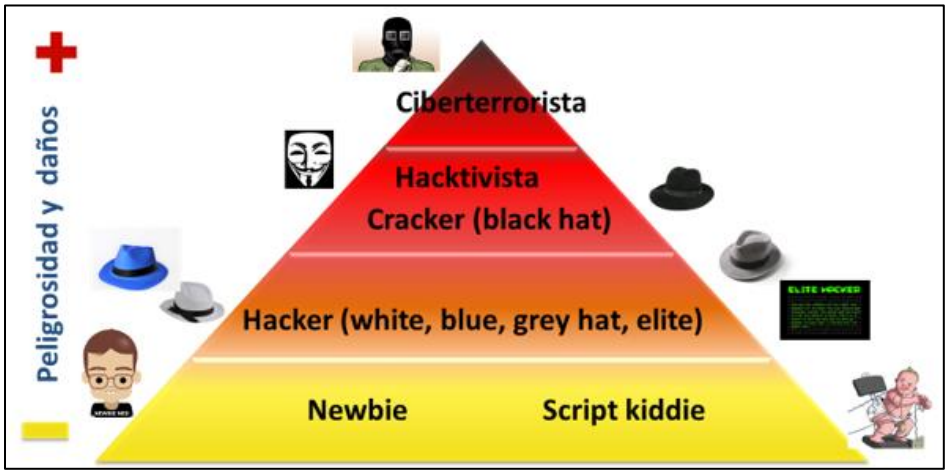
- **Hacker:** Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. Dentro de esta categoría se encuentran las personas que, utilizando sus conocimientos, acceden ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta. A estos últimos también se les conoce como piratas informáticos.[10]

    - **Tipología de hackers[11]:**
        - **Hacker de sombrero negro:** Es una persona que intenta obtener una entrada no autorizada en un sistema o red para explotarlos por razones maliciosas. El hacker de sombrero negro no tiene ningún permiso o autoridad para llevar a cabo sus objetivos. Intenta infligir daños al comprometer los sistemas de seguridad, alterar las funciones de los sitios web y las redes, o apagar los sistemas.
        - **Hacker de sombrero blanco:** El hacker del sombrero blanco es buena gente. Se les llama también hackers éticos porque prueban las infraestructuras de Internet existentes para investigar las lagunas en el sistema. Crean algoritmos y realizan múltiples metodologías para entrar en sistemas, solo para fortalecerlos.
        - **Hacker de sombrero gris:** Se mueve entre los de sombrero negro y blanco. Si bien no pueden usar sus habilidades para beneficio personal, pueden, sin embargo, tener buenas y malas intenciones. Por ejemplo, un hacker que piratea una organización y encuentra cierta vulnerabilidad puede filtrarla a través de Internet o informar a la organización al respecto.
        - **Hacker de sombrero azul:** Su misión es perfeccionar software inédito. Son contratados para probar el

[9] Disponible en: https://www.iwomanish.com/papa-que-es-un-hacker-y-un-cracker-techcheck-sobre-seguridad-en-internet/.
[10] Disponible en: https://dle.rae.es/j%C3%A1quer#TLIznqw.
[11] Disponible en: https://www.muyinteresante.es/tecnologia/articulo/que-es-un-hacker-de-sombrero-gris-831473842564.

software en busca de errores antes de su lanzamiento.

- **Script kiddie:** Esta subcategoría de hacker representa a hackers novatos que no están calificados. Dependen de programas y archivos para hackear y no se molestan en aprender cómo funcionan. Tienen poco respeto por las habilidades y no están motivados para aprender. Los Script Kiddies pueden ser de sombrero blanco, sombrero negro o gris.
- **Newbie:** Se refiere a los "novatos del hacking" y que, por esa razón, no poseen casi ningún conocimiento o experiencia en el mundo de la tecnología.[12]



[12] Disponible: https://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027.

Ejemplos típicos de las amenazas y consecuencias

De acuerdo con la **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales** del INAI, una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Estas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas y además provenir de adentro o desde afuera de la organización. A continuación, se presentan unas tablas con algunos ejemplos de amenazas que son identificados en la Guía referida.

a) Por origen

- **Origen humano:** Son aquellas que son ocasionadas por el ser humano.

Origen de la amenaza	Motivación / causa
Hacker, cracker	• Desafío • Dinero • Ego • Estatus • Rebelión
Criminal computacional	• Alteración no autorizada de información • Destrucción de información • Ganancia económica • Revelación ilegal de información
Terrorista	• Chantaje • Destrucción • Explotación • Ganancia política • Reconocimiento mediático • Venganza
Espía industrial (inteligencia empresarial, gobiernos extranjeros, robo de tecnología, etc.)	• Espionaje económico • Ventaja competitiva

Interno (Personal con poco entrenamiento, descontento, negligente, deshonesto o empleados despedidos)	• Curiosidad • Ego • Errores no intencionales u omisiones (por ejemplo, errores de captura de información, errores de programación) • Ganancia económica • Venganza

- **Origen natural:** Son aquellas en las que no interviene, al menos de manera directa, el ser humano.

Ejemplos:
- Fenómenos climáticos o meteorológicos (tornado, inundación, huracán)
- Fenómenos sísmicos
- Fenómenos volcánicos

b) Por tipo

Tipo	Amenazas
Daño Físico	• Fuego • Agua • Contaminación • Accidentes • Polvo, corrosión, humedad, congelamiento
Eventos naturales	• Fenómenos climáticos o meteorológicos • Fenómenos sísmicos • Fenómenos volcánicos
Pérdida de servicios básicos	• Falla en el sistema de aire acondicionado o suministro de agua • Pérdida de suministro eléctrico • Falla en los equipos de telecomunicaciones
Información comprometida por fallas técnicas	• Intercepción e interferencia de señales • Espionaje remoto • Escucha en comunicaciones

	• Robo de medios o documentos • Robo de equipo • Recuperación de medios desechados o reciclados • Revelación • Fuentes poco confiables para la obtención de datos • Alteración de hardware • Alteración de software • Rastreo de localización • Fallas del equipo • Malfuncionamiento del equipo • Saturación de los sistemas de información • Malfuncionamiento del software • Falla en el mantenimiento del sistema de información
Acciones no autorizadas	• Uso no autorizado de equipo • Uso de software copiado o falsificado • Corrupción de datos • Procesamiento ilegal de los datos
Compromiso de las funciones	• Error de uso • Abuso de privilegios • Falsificación de privilegios • Denegación de acciones

Consecuencias de las amenazas a los dispositivos

a) Daños a los activos

Los daños a los activos tienen consecuencias diferenciadas en función del origen de la amenaza, sobre todo en el caso de las que son consecuencia de acciones humanas, pues los motivos que se persiguen son diferentes en cada caso concreto. Sin embargo, para sistematizar la información, a continuación, se presenta una tabla con las posibles consecuencias de diversas amenazas a la seguridad de los datos personales.

Origen de la amenaza	Posibles consecuencias
Hacker, cracker	• Acceso no autorizado al sistema • Ingeniería social • Intrusión en los sistemas • Robo de información
Criminal computacional	• Acciones fraudulentas, robo • Extorción y chantaje, acoso • Intrusión a los sistemas informáticos • Sobornos de información • Suplantación de identidad • Venta de información personal
Terrorista	• Ataque a personas y/o instalaciones (por ejemplo, bomba) • Ataque a sistemas (por ejemplo, denegación de servicio) • Manipulación de los sistemas • Penetración a los sistemas
Espía industrial (inteligencia empresarial, gobiernos extranjeros, robo de tecnología, etc.)	• Acceso no autorizado a información clasificada o propietaria • Explotación económica • Ingeniería social • Intrusión a la privacidad del personal • Penetración a los sistemas

Interno (personal con poco entrenamiento, descontento, negligente, deshonesto o empleados despedidos)	• Abuso en la operación de los sistemas • Acceso no autorizado a los sistemas • Ataque a empleados y/o instalaciones • Chantaje • Código malicioso • Consulta de información clasificada o propietaria • Datos incorrectos o corruptos • Errores en los sistemas • Fraude y robo • Intercepción de comunicaciones • Intrusiones a sistemas • Sabotaje de los sistemas • Sobornos de información • Venta de información personal

b) *Vulneraciones a la seguridad de datos personales*

En materia de seguridad de la información, una de las principales consecuencias de las amenazas, sobre todo de las de origen humano, son las vulneraciones de datos personales.

Ejemplos:
De acuerdo con el artículo 63 del **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

- La pérdida o destrucción no autorizada de datos personales.
- El robo, extravío o copia no autorizada de datos personales.
- El uso, acceso o tratamiento no autorizado de datos personales.
- El daño, la alteración o modificación no autorizada de datos personales.

Si se observa como una cadena de hecho, se puede afirmar que las vulneraciones de seguridad son incidentes de seguridad que

involucran datos personales, las cuales podrían resultar en revelaciones de información.

En el módulo 3 se revisará con mucho mayor detalle todo lo relacionado con las vulneraciones a la seguridad de datos personales.

Materiales de difusión

Artículos de interés

- Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.
- Guía para Prevenir el Robo de Identidad.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Examen de evaluación

1. **Es cualquier valor para la organización que requiera ser protegido. En el caso de la seguridad de los datos personales, deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Los activos se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo.**

   a) Activos
   b) Hardware
   c) Software
   d) Hacker
   e) Ninguna de las anteriores

2. **¿Qué es un incidente de seguridad?**

   a) 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
   b) Cualquier evento o circunstancia que han provocado o podrían haber provocado un daño innecesario a un titular de los datos
   c) Cualquier evento o circunstancia que afecte la seguridad pública
   d) Cualquier problema suscitado en el ámbito laboral que pone en riesgo a los trabajadores
   e) Ninguna de las anteriores

3. **¿Cuál es el orden correcto del ciclo de vida de los datos personales?**

   a) Obtención, uso, almacenamiento, divulgación, cancelación y bloqueo
   b) Obtención, almacenamiento, uso, divulgación, bloqueo y cancelación

c) Obtención, uso, divulgación, almacenamiento, bloqueo y cancelación
d) Obtención, almacenamiento, bloqueo, uso, divulgación y cancelación
e) Obtención, bloqueo, cancelación, uso, divulgación y almacenamiento

4. **Es una técnica utilizada para obtener información de las personas teniendo como base la interacción social, la manipulación y el engaño, y ocurre típicamente en conversaciones directas entre el delincuente y la víctima**

a) Fraude comunicacional
b) Cibercrimen
c) Pirateo
d) Ingeniería social
e) Ninguna de las anteriores

5. **A una persona cuya misión es perfeccionar software inédito y que además es contratada para probar el software en busca de errores antes de su lanzamiento se le conoce como:**

a) Hacker de sombrero blanco
b) Hacker de sombrero gris
c) Hacker de sombrero negro
d) Hacker de sombrero azul
e) Hacker de sombrero amarillo

6. **Las amenazas que tiene el potencial de dañar un activo y causar una vulneración a la seguridad se clasifican por:**

a) Tipo de usuario al que afectan
b) Duración del daño
c) Origen y tipo
d) Todas las anteriores
e) Ninguna de las anteriores

7. **Son ejemplos de amenazas de origen natural**

a) Fenómenos climáticos o meteorológicos
b) Fenómenos sísmicos
c) Fenómenos volcánicos
d) Todas las anteriores
e) Ninguna de las anteriores

8. **En materia de seguridad de la información, ¿cuál es la principal consecuencia de las amenazas, sobre todo las de origen humano?**

a) Extorsión y chantaje
b) Vulneraciones a la seguridad de los datos personales
c) Abuso en la operación de los sistemas
d) Explotación económica
e) Errores en los sistemas

9. **Son posibles consecuencias de una amenaza provocada por un hacker o un cracker:**

a) Ingeniería social
b) Intrusión en los sistemas
c) Robo de información
d) Todas las anteriores
e) Ninguna de las anteriores

10. **Un incidente de seguridad que involucra datos personales se denomina:**

a) Usurpación de identidad
b) Vulneración de seguridad
c) Revelación de información no autorizada
d) Revelación ilegal de información
e) Ninguna de las anteriores