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

MÓDULO 2. Amenazas

1

Conceptos

- Activos
- Amenaza
- Ciclo de vida de los datos personales
- Vulnerabilidad
- Incidente de seguridad
- Vulneración de seguridad
- Ingeniería social
- Terrorista informático
- Hacktivista
- Cracker
- Hacker

2

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.

3

Conceptos

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.

Conceptos

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**.

Conceptos

Vulnerabilidad

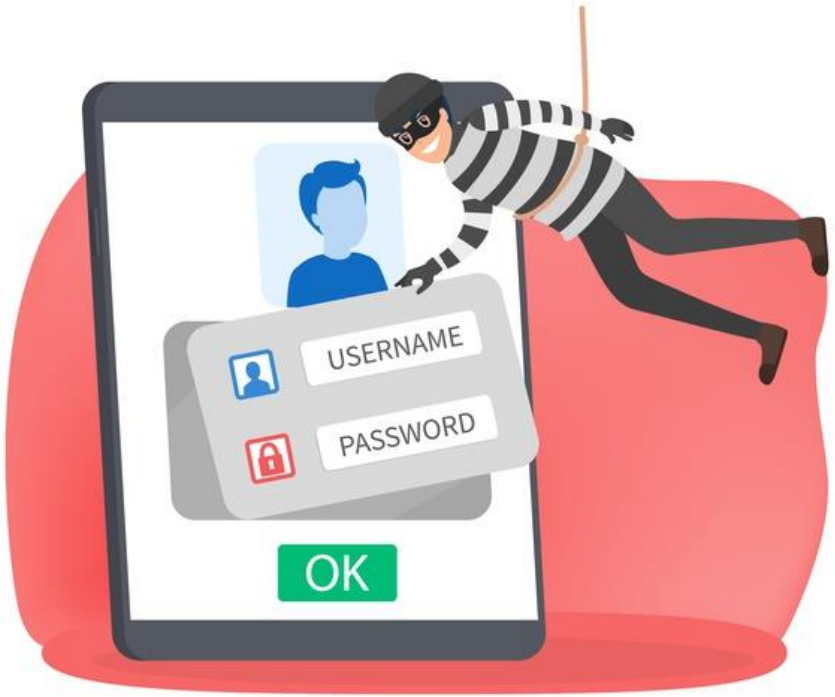
Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Conceptos

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.

Conceptos



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.

Conceptos

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.

Conceptos

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).

Conceptos

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.

Conceptos

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.

Conceptos

Cracker

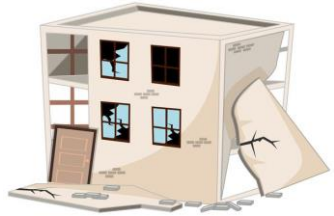
Los **crackers o hackers de sombrero negro** son esas personas que usan todo su talento y conocimiento no para el bien sino para **romper sistemas informáticos o entrar de forma ilícita en sistemas informáticos**; esto es un delito y eso hay que tenerlo muy claro.

Ejemplos típicos de las amenazas y consecuencias

Una **amenaza** tiene el potencial de dañar un activo y causar una vulneración a la seguridad de la información y de los datos personales.

Las amenazas pueden ser:

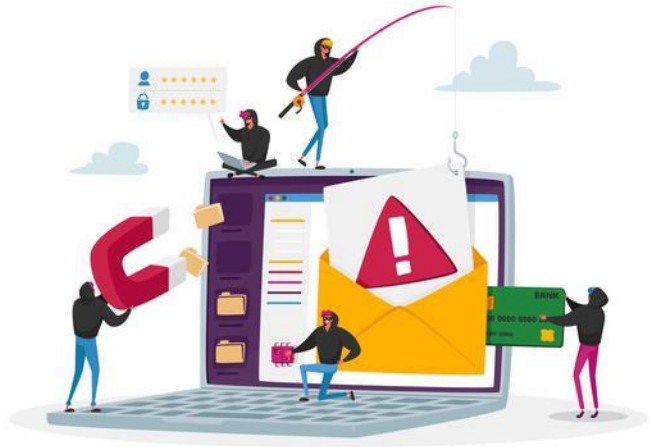
- **De origen natural:** Fenómenos climáticos o meteorológicos; fenómenos sísmicos o fenómenos volcánicos.



- **De origen humano:** Hackers, criminales computacionales, terroristas, espías industriales.

Consecuencias de las amenazas a los dispositivos

- Daños a los activos.
- **Vulneraciones a la seguridad de datos personales**:
    - Pérdida o destrucción no autorizada de datos personales.
    - Robo, extravío o copia no autorizada de datos personales.
    - Uso, acceso o tratamiento no autorizado de datos personales.
    - Daño, la alteración o modificación no autorizada de datos personales.



Gracias por su atención