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

MÓDULO 3. Vulneraciones a la seguridad de datos personales

inai

1

¿Qué es una vulneración a la seguridad de los datos personales?

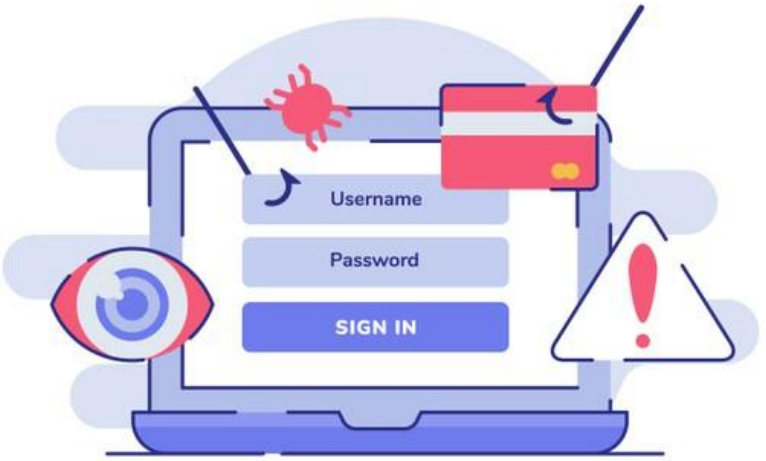
El Reglamento de Ley Federal de Protección de Datos Personales en Posesión de los Particulares define en el artículo 63 una vulneración como:

1.- La **pérdida o destrucción no autorizada de los datos**

2.- El **robo, extravío o copia no autorizada**

3.- Su **uso, acceso o tratamiento no autorizado**

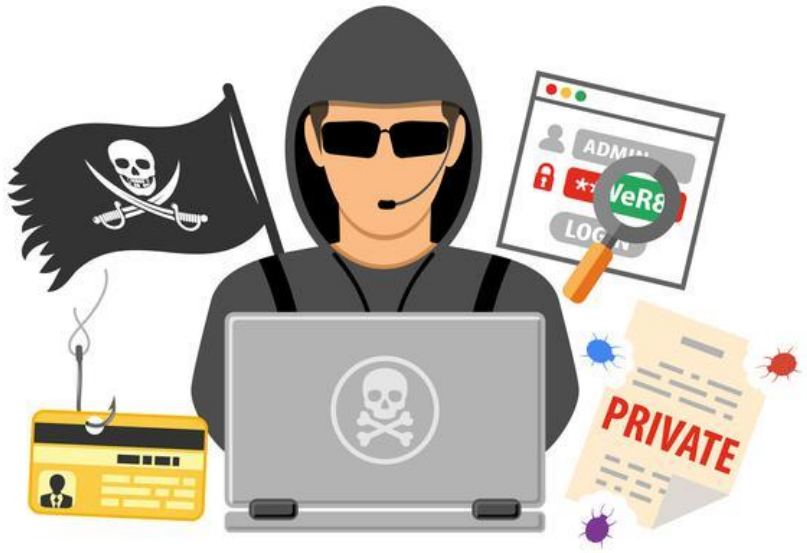
4.- El **daño, la alteración o su modificación no autorizada**



PASSWORD PHISING

2

Tipo de vulneraciones

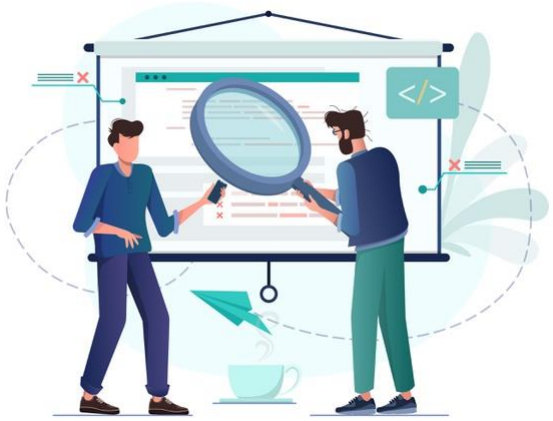


- **Confidencialidad:** produce una **revelación o acceso** no autorizada o accidental de los datos personales.
- **Disponibilidad:** produce una **pérdida de acceso o destrucción** accidental o no autorizada a los datos personales.
- **Integridad:** produce una **alteración no autorizada o accidental** de los datos personales.

3

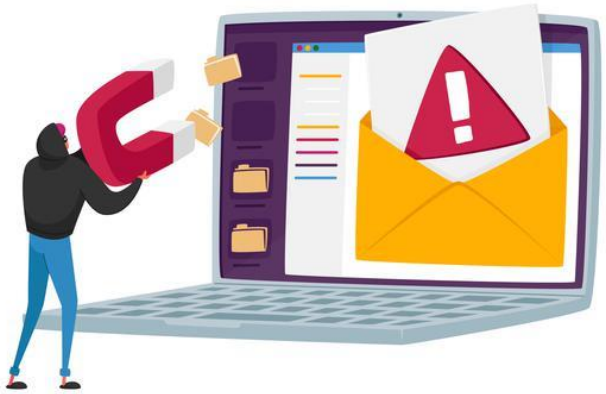
Fases de una vulneración a la seguridad de los datos personales

Etapas generales de vulneración:



Investigación

Ataque

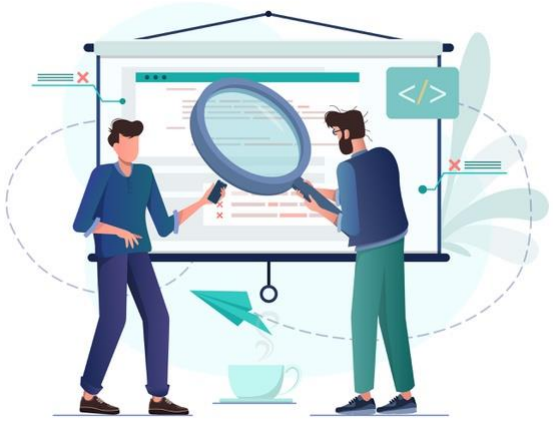


Exfiltración de datos

4

Fases de una vulneración a la seguridad de los datos personales

Etapas generales de vulneración:



Investigación

Una vez elegido el objetivo, el **atacante busca los puntos débiles que puede explotar**: empleados, sistemas o la red.

Esto **implica largas horas de investigación por parte del atacante** y puede implicar el acecho de los perfiles de las redes sociales de los empleados para averiguar qué tipo de infraestructura tiene la empresa.

5

Fases de una vulneración a la seguridad de los datos personales

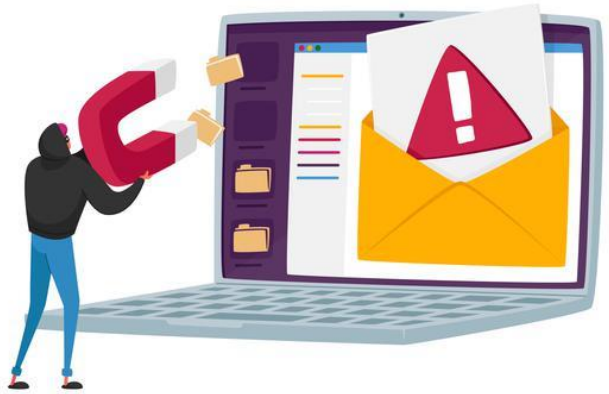
Etapas generales de vulneración:

Detectados los puntos débiles del objetivo, el **atacante establece el primer contacto**.

Ataque

Fases de una vulneración a la seguridad de los datos personales

Etapas generales de vulneración:



Exfiltración de datos

Una vez dentro de la red, el atacante es libre de **extraer información**, siendo los datos personales el recurso más atractivo.

Estos datos pueden utilizarse para el **chantaje o la ciberpropaganda**.

Actores relevantes ante una vulneración a la seguridad de los datos personales

Responsable de Tratamiento:

Debe de informar inmediata a las personas titulares las vulneraciones

Persona o departamento de datos personales:

Debe informar y asesorar al responsable del tratamiento sobre las obligaciones y responsabilidades establecidas en el marco legal

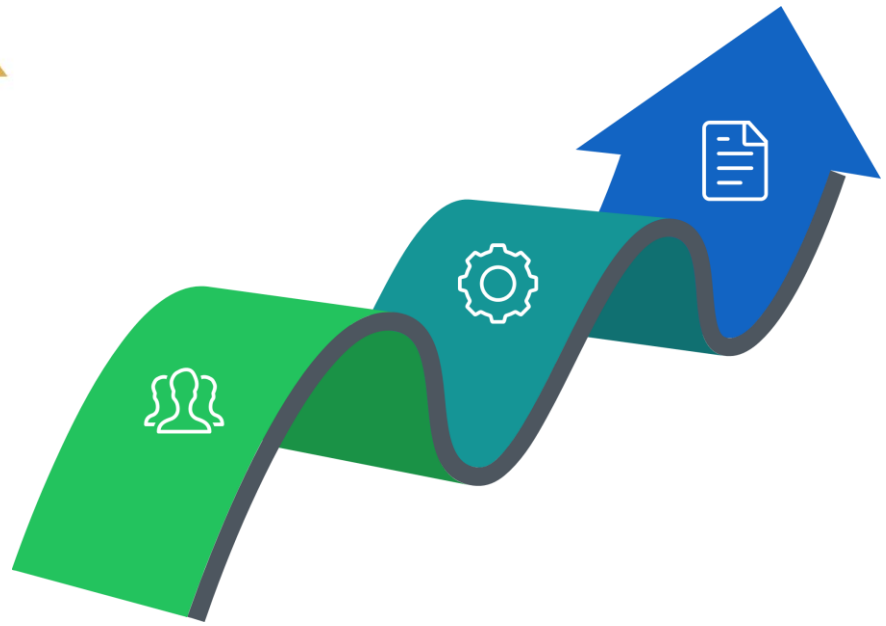
Encargado:

Deberá informar al responsable del tratamiento cuando se presente una vulneración a los datos personales que trata

8

Gestión de vulneraciones de seguridad de datos personales

Plan de respuesta a incidentes de seguridad de datos personales



1. **Preparación:** desarrollar y mantener políticas, controles de seguridad que permitan actuar ante los incidentes de seguridad planteados anteriormente.

2. **Identificación:** en esta etapa se detectan las alertas de seguridad y se determina si éstas son incidentes.

3. **Contención:** esta etapa consiste en limitar el alcance o impacto del incidente identificado.

4. **Mitigación:** Tratamiento profundo del incidente de seguridad para minimizar la posibilidad de que éste se repita.

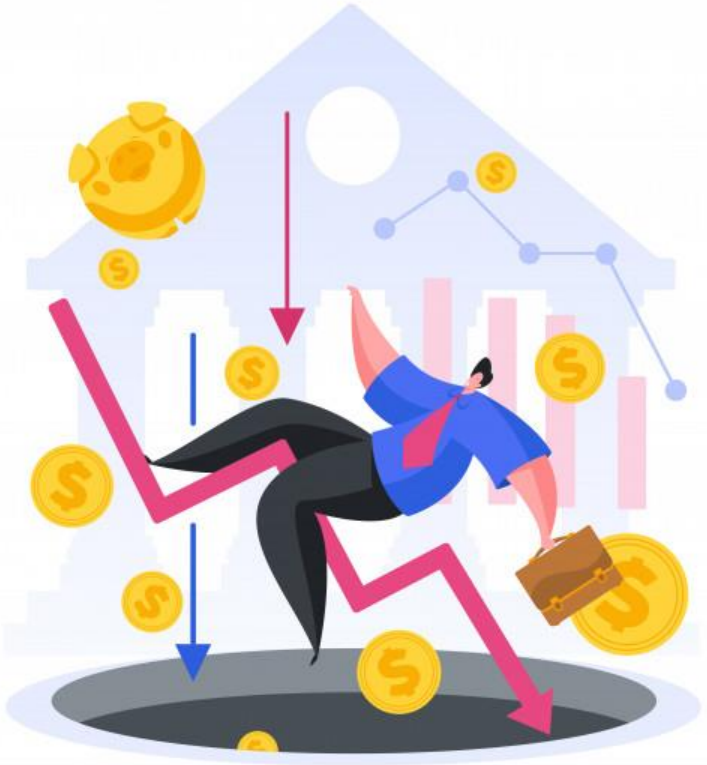
5. **Recuperación:** seguimiento a las medidas implementadas en la mitigación, activos afectados se reintegran a los sistemas de tratamiento.

6. **Mejora continua:** completar la documentación de lo que se hizo respecto al incidente, se comunica a las partes interesadas y se elabora la bitácora.

Consecuencias de una vulneración a la seguridad de los datos personales

Consecuencias para los responsables

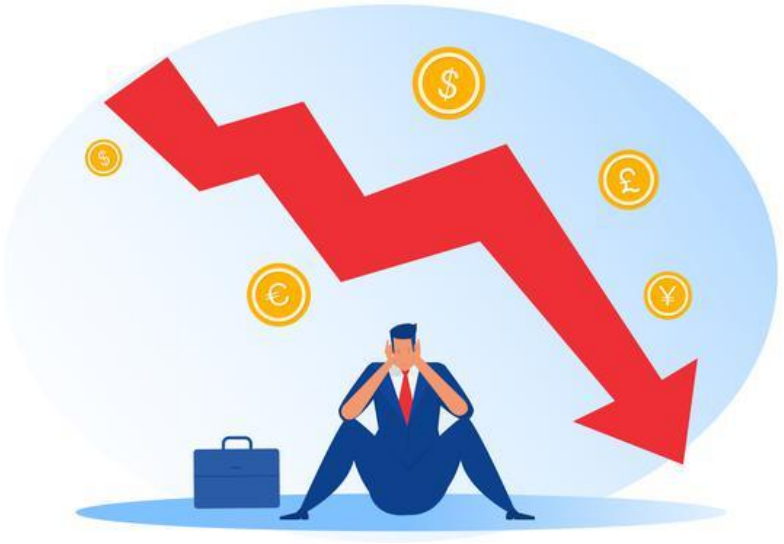
a) Multas y sanciones por la autoridad.
b) Pérdida de confianza y clientes.
c) Daño reputacional.
d) Impacto financiero.
e) Pérdida de socios de negocio.



10

Consecuencias de una vulneración a la seguridad de los datos personales

Consecuencias para los encargados



a) Sanciones por el responsable del tratamiento.
b) Pérdida de confianza y clientes.
c) Daño reputacional.
d) Impacto financiero.
e) Pérdida de clientes.

Consecuencias de una vulneración a la seguridad de los datos personales

Consecuencias para los titulares

a) Pérdidas financieras.

b) Fraude.

c) Víctima de campañas de phishing/spamming.

d) Daños psicológicos o físicos.

e) Uso no autorizado de cuentas y/o datos personales.

f) Discriminación.

g) Daño a la reputación, al honor o la integridad física de las personas titulares.

h) Pérdida de control sobre sus datos personales.

i) Tratamiento indebido de datos personales.

Gracias por su atención