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

MÓDULO 3. Vulneraciones a la seguridad de datos personales

Índice

¿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[1] una vulneración como:

- La **pérdida o destrucción no autorizada de los datos**, por ejemplo, que un empleado descontento con acceso al archivo que resguarda los expedientes de los empleados de la organización destruya sin autorización documentos que contienen datos personales.
- El **robo, extravío o copia no autorizada** de los mismos, por ejemplo, que un empleado realice una copia no autorizada en una usb, de una base de datos personales almacenada en el equipo de cómputo de su compañero de trabajo.
- Su **uso, acceso o tratamiento no autorizado**, por ejemplo, que un área dentro de la organización realice un evento utilizando los datos personales de contacto que otra área recabo, sin una autorización previa para utilizarlos.
- El **daño, la alteración o su modificación no autorizada**, por ejemplo, que un software malicioso dañe la base de datos personales al infectar el sistema informático en donde la información se procesa.

a) Definición

Es común que cuando se define una vulneración a la seguridad de datos personales sea utilizado el término de **incidente de seguridad**; sin embargo, no significan lo mismo, dado que el primero se refiere 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[2] mientras que las **vulneraciones a la seguridad de datos personales** son un tipo particular de incidentes de seguridad que pueden ocurrir en

[1] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

[2] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones_Manejo_IS_DP.pdf

cualquier fase del tratamiento de datos personales y se caracterizan por:

Afectar a los **sistemas de tratamiento**	Afectar los **derechos patrimoniales o morales** de los titulares de datos personales

b) Tipos de vulneraciones a la seguridad de los datos personales

- **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.

c) Actores y motivaciones

De acuerdo con el informe **Data Breach Report 2021 de Verizon**[3] la motivación financiera sigue siendo la causa más común de ataques y los principales actores continúan siendo los actores externos, el crimen organizado y los actores internos.

d) Tácticas más comunes

El informe de **Verizon**[4] refiere que la técnica más utilizada para las vulneraciones a la seguridad datos personales son el hacking[5], errores, ataques de ingeniería social y software malicioso principalmente.

[3] Disponible en: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[4] https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

[5] El **hacking se** puede definir como "la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes". En otras palabras, el hacking consiste en la detección de vulnerabilidades de seguridad, y también engloba la explotación de las mismas.

Fases de una vulneración a la seguridad de los datos personales

Si bien existen diferentes formas de realizar una vulneración a la seguridad de los datos personales, es posible distinguir tres etapas generales[6], a saber:

- **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.

- **Ataque:** Detectados los puntos débiles del objetivo, el atacante establece el primer contacto de dos maneras:

    - Ataque basado en la red: el atacante explota las debilidades de la infraestructura del objetivo para provocar una vulneración. Estos puntos débiles pueden incluir, entre otros, la infiltración de un código intruso (inyección SQL)[7], la explotación de vulnerabilidades y/o el secuestro de sesiones[8].
    - Ataque social: el atacante utiliza tácticas de ingeniería social[9] para infiltrarse en la red objetivo.

- **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. La información que un

[6] Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/data-breach
[7] La inyección SQL, o SQLi, es un tipo de ataque a una aplicación web que permite a un atacante insertar sentencias SQL maliciosas en la aplicación web, obteniendo potencialmente acceso a datos sensibles en la base de datos o destruyendo estos datos
[8] *Session Hijacking* (secuestro o robo de sesión) se refiere a que un individuo (atacante) consigue el identificador de sesión entre una página web y un usuario, de forma que puede hacerse pasar por este y acceder a su cuenta en esa página web.
[9] La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con *malware* o abran enlaces a sitios infectados.

atacante recopila también puede utilizarse para ejecutar ataques más dañinos contra la infraestructura del objetivo.

Obligaciones de los responsables ante una vulneración a la seguridad de los datos personales.

Las vulneraciones a la seguridad de los datos personales, además de poner en riesgo la intimidad y la privacidad de las personas titulares de los datos, con las consecuencias que podrían derivar en función del uso que se haga de ellos, también supone un costo en términos económicos para los responsables del tratamiento.

De acuerdo con el "Informe del costo de las vulneraciones de datos 2020" de IBM, el costo promedio total de una vulneración asciende a **3.86 millones de dólares**[10]. Esto incluye una combinación de costos directos e indirectos relacionados con el tiempo y el esfuerzo para hacer frente a una vulneración, las oportunidades perdidas, como la pérdida de clientes como resultado de la mala publicidad, y las multas reglamentarias.

Otro costo asociado con una vulneración se relaciona con el tiempo que transcurre entre su identificación y su contención, el cual, de acuerdo con el mismo informe, es de **280 días** en promedio.

Para el cumplimiento de las obligaciones derivadas de una vulneración a la seguridad de los datos personales es necesario identificar los actores relevantes y su participación:

- ***Responsable del tratamiento***, debe informar de forma inmediata a las personas titulares las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecte de forma significativa sus derechos patrimoniales o morales, a fin de que puedan tomar las medidas correspondientes para la defensa de sus derechos.

[10] Disponible en: https://www.ibm.com/security/digital-assets/cost-data-breach-report/?utm_medium=OSocial&utm_source=Blog&utm_content=000039JJ&utm_term=10013747&utm_id=SI-blog-1&cm_mmc=OSocial_Blog-_-Portfolio%20Security_Security%20Conversation-_-WW_WW-_-SI-blog-1_ov76748&cm_mmca1=000039JJ&cm_mmca2=10013747#/es-mx

La notificación deberá realizarse, en cuanto el responsable confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación.

Adicionalmente el responsable, deberá analizar las causas por las cuales se presentó la vulneración e implementar las acciones correctivas, preventivas, a efecto de evitar que la vulneración se repita.

- ***Persona o departamento de datos personales***, debe informar y asesorar al responsable del tratamiento sobre las obligaciones y responsabilidades establecidas en el marco legal en la materia sobre las vulneraciones a la seguridad de los datos personales.

  Esta figura deberá actuar como el punto de contacto entre las personas titulares y el responsable durante el proceso de notificación de la vulneración a la seguridad de los datos personales.

  Adicionalmente, deberá atender los requerimientos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que es la autoridad en materia de protección de datos personales, en las cuestiones relativas a la gestión de la vulneración de seguridad de datos personales.

- ***Encargado***, deberá informar al responsable del tratamiento cuando se presente una vulneración a los datos personales que trata, además debe brindar ayuda al responsable para la gestión de la vulneración de tal forma que el responsable pueda cumplir con las obligaciones establecidas por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

A continuación, se presentan las obligaciones que deberán cumplir los responsables del tratamiento de datos personales, con base en lo establecido en el marco legal mexicano en materia de protección de datos personales ante una vulneración a la seguridad de los datos.

La **Ley Federal de Protección de Datos Personales en Posesión de los Particulares** para el sector privado (LFPDPPP) en el artículo 20, establece la obligación para las y los responsables del tratamiento de datos personales de realizar una notificación a las y los titulares, en cuanto se confirme que ocurrió una vulneración a la seguridad de sus datos personales que afecte de forma significativa sus **derechos patrimoniales o morales**.

Los ***derechos patrimoniales*** están relacionados de forma enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica de las y los titulares.

Por su parte los ***derechos morales*** se refieren 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.

La ***notificación a las y los titulares deberá*** al menos incluir los siguientes elementos:

a) La naturaleza del incidente.
b) Los datos personales comprometidos.
c) Las recomendaciones a las personas titulares acerca de las medidas que éste pueda adoptar para proteger sus intereses.
d) Las acciones correctivas realizadas de forma inmediata y
e) Los medios donde pueden las personas titulares obtener más información al respecto.

La notificación a personas titulares cuando ha ocurrido una vulneración a la seguridad de los datos personales además de ser una obligación para los responsables realizarla puede traer grandes **beneficios para la organización**:

- Limita el mal uso de datos personales, permite a las personas titulares tomar acciones para su protección.
- Minimiza la pérdida de confianza de las personas titulares.
- Puede reducir costos de mitigación, evitar denuncias, sanciones.

Es importante que los responsables realicen la notificación de la vulneración en el menor tiempo posible, cuando ya tenga la información concreta sobre la misma y no exista exposición de los activos involucrados.

Asimismo, los responsables del tratamiento de datos personales deberán implementar ***medidas preventivas y correctivas*** mediante las cuales analicen las causas por las cuales se presentó la vulneración y establecer un plan de trabajo que incluya acciones preventivas y correctivas para en su caso adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Adicionalmente, deberán **evaluar el riesgo de una vulneración de seguridad de datos personales**, considerando:

a) Tipo de vulneración de seguridad de datos personales.
b) Sensibilidad de los datos personales involucrados en la vulneración.
c) Facilidad de identificar a las personas titulares afectados por la vulneración de seguridad de datos personales.
d) Impacto de la afectación a los derechos morales o patrimoniales de las personas titulares de los datos personales.
e) Número de personas titulares afectados.
f) Incumplimiento con marcos normativos que deba considerar el responsable.

Gestión de vulneraciones de seguridad de datos personales

El INAI ha publicado el documento **Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales**[11] con el objetivo de describir los procesos y controles recomendados por el Instituto para generar un plan de respuesta a incidentes de seguridad, en participar para mitigar las vulneraciones a la seguridad de los datos personales. Estas recomendaciones ayudan y orientan a los responsables para:

a) Reconocer las diferencias entre alertas e incidentes de seguridad.
b) Elaborar un plan para responder ante incidentes de seguridad, conforme estándares internacionales.
c) Utilizar formatos de referencia para documentar los incidentes de seguridad.

El documento presenta la propuesta de un **plan de respuesta a incidentes de seguridad de datos personales** integrado por seis etapas:

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.

[11] Disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Adicionalmente existen **estándares y buenas prácticas** que los responsables pueden adoptar para la gestión de las vulneraciones a la seguridad de los datos personales, algunas de ellas se presentan a continuación:

- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales – INAI.
- Guía para la gestión y notificación de brechas de seguridad- Agencia Española de Protección de Datos.
- Incident Handler's Handbook SANS Institute.
- Computer Security Incident Handling Guide NIST.
- ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.
- ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- A Practical Guide to Personal Data Breach Notifications under the GDPR.
- Personal data breaches – Information Commissioner´s Office
- Guidelines 01/2021 on Examples regarding Data Breach Notication.
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.

Consecuencias de una vulneración a la seguridad de los datos personales

Las ***consecuencias para los responsables*** **de** una vulneración de datos personales son:

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.

a) Encargados

Las ***consecuencias de una vulneración de datos personales para un encargado*** pueden ser:

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

b) Las personas titulares

Las ***consecuencias*** de una vulneración de datos personales para las personas ***titulares*** son:

a) Pérdidas financieras.
b) Fraude.
c) Víctima de campañas de phishing[12]/spamming[13].

[12] **Phishing:** Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar

[13] **Spamming:** Acción de enviar correo no deseado, correo basura o no solicitado.

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.

El INAI es la autoridad garante del derecho a la protección de datos personales, por lo tanto, se puede acudir ante esta autoridad cuando las personas titulares tengan conocimiento de un tratamiento indebido de los datos personales, y hacer uso de los procedimientos señalados en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Ahora bien, es importante definir qué se entiende por **tratamiento indebido de datos personales.** Al respecto, se deben considerar diversos factores, entre ellos: el uso ilícito, la divulgación no permitida o el almacenamiento excesivo y desproporcionado de los datos personales, que lleve a cabo el responsable de su protección, sea cual sea el medio físico o electrónico.

Es importante reiterar que ***el INAI no está facultado para investigar el robo de identidad***, pues la persecución de este delito corresponde a la autoridad penal**. *No obstante, el Instituto puede investigar el indebido tratamiento de datos personales vinculados con el robo de identidad, como, por ejemplo, la falta de medidas de seguridad para la protección de los datos personales*.**

j) Robo de identidad

Es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso no autorizado e ilegal de datos personales[14].
El robo de identidad puede tener consecuencias graves para las personas titulares de los datos personales, que pueden requerir de

[14] Disponible en: https://micrositios.inai.org.mx/identidadsegura/?page_id=37

tiempo y recursos económicos para resolverse. Algunos ejemplos de posibles ***daños*** son:

- ***Contratar créditos o servicios a tu nombre***, lo que puede dañar tu historial crediticio o afectar tu patrimonio.
- ***Acceder a tus cuentas bancarias*** y causarte un daño económico importante.
- ***Hacer publicaciones en Internet a tu nombre***, o enviar información a tu lista de contactos y ***dañar tu imagen*** pública y tu reputación.

Numerología del robo de identidad

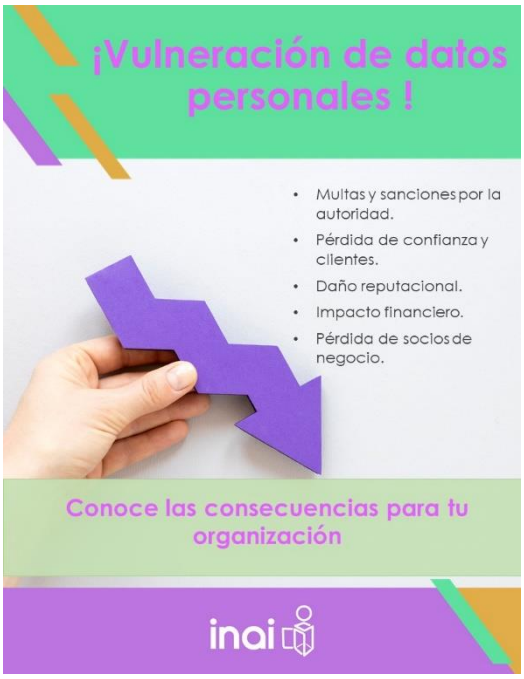
- Según el Termómetro de Privacidad 2014 de Deloitte[15], ***en México los elementos más susceptibles*** a vulneraciones de seguridad relacionadas con el robo de identidad son: 1) Robo o fuga a través de correo electrónico, y 2) robo de información en dispositivos portátiles, tales como memorias USB, celulares o tabletas.
- De acuerdo con datos del Banco de México[16] y firmas especializadas[17], ***nuestro país ocupa el 8° lugar en este delito en el mundo y el 2° lugar en América Latina***[18], 67% es por pérdida de documentos, 63% por robo de una cartera y portafolios y 53% es información tomada de una tarjeta bancaria.
- ***9 de cada 10 personas llevan información suficiente en su cartera para ser víctima de robo de identidad*** según cifras de CPP México[19], el 86% lleva en su cartera la credencial para votar, el 49% la tarjeta de débito, el 30% la licencia de conducir, 27% tarjetas departamentales y 17% tarjetas de crédito[20].

[15] Disponible en: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Termometro_2daEd_2014.pdf
16 Disponible en: http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad
17 Disponible en: https://www.eleconomista.com.mx/finanzaspersonales/Evite-llevar-toda-su-identidad-en-la-cartera-20130207-0024.html
[18] Disponible en: https://mexico.cppdirect.com/identity-protection#InformaciónImportante
[19] Disponible en: https://mexico.cppdirect.com/identity-protection#InformaciónImportante
[20] Disponible en: http://m.aristeguinoticias.com/2901/mexico/inai-exige-facultades-para-perseguir-robo-de-identidad/

- Según el Estudio sobre los hábitos de los usuarios de internet en México 2021[21] de la Asociación de Internet.mx, entre los usos personales o de ocio de los mexicanos, destaca acceder a redes sociales (cerca del 86.8%), en donde ***dejan datos personales que permiten a los atacantes inferir contraseñas, preguntas de seguridad u otras credenciales de autenticación.***

[21] Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v15%20Publica.pdf

Materiales de difusión



Consulta

Las recomendaciones que el INAI ha publicado para el Manejo de Incidentes de Seguridad de Datos Personales

Artículos de interés

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales – INAI.
- Guía para la gestión y notificación de brechas de seguridad- Agencia Española de Protección de Datos.
- Incident Handler's Handbook SANS Institute.
- Computer Security Incident Handling Guide NIST.
- ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.
- ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.
- A Practical Guide to Personal Data Breach Notifications under the GDPR.
- Personal data breaches – Information Commissioner´s Office
- Guidelines 01/2021 on Examples regarding Data Breach Notication.
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679.

Examen de evaluación

1. **Las vulneraciones a la seguridad de personales son un tipo particular de _____ que pueden ocurrir en cualquier fase del tratamiento de datos personales**
   a) Incidente de seguridad
   b) Alerta de seguridad
   c) Brecha de seguridad
   d) Violación de seguridad
   e) Ninguna de las anteriores

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

   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) Pérdida o destrucción no autorizada de los datos, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado, daño, la alteración o su modificación no autorizada.
   c) Cualquier problema suscitado en el ámbito laboral que pone en riesgo a los trabajadores y sus datos personales.
   d) Ninguna de las anteriores

3. **Fases de una vulneración a la seguridad de los datos personales**

   a) Investigación, ataque, extracción de datos
   b) Investigación, análisis, exfriltración de datos
   c) Investigación, ataque, cifrado de datos
   d) Investigación, ataque, exfriltración de datos

4. **Actores relevantes que participan en la gestión de una vulneración a la seguridad de datos personales**

   a) Responsable del tratamiento, oficial de PDP, personal o departamento de datos personales y encargado.

b) Responsable del tratamiento, autoridad de protección de datos personales, personas titulares y encargados.
c) Responsable, encargado y tercero.
d) Responsable y tercero.

5. **Los _____están relacionados de forma enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.**

a) Derechos financieros
b) Derechos patrimoniales
c) Derechos morales
d) Derechos materiales

6. **Los _____ se refieren 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.**

a) Derechos humanos
b) Derechos patrimoniales
c) Derechos personales
d) Derechos morales

7. **Los _____ del tratamiento de datos personales deberán evaluar el riesgo de una vulneración de seguridad de datos personales.**

a) terceros
b) encargados
c) responsables
d) titulares

8. **Los _____ tienen la obligación según lo establecido en el artículo 39 de la LGPDPPSO de llevar una bitácora de las vulneraciones a la seguridad en la que se describan, la fecha en la que ocurrió, el monto de éstas y las acciones correctivas implementadas de forma inmediata y definitiva.**

   a) terceros
   b) titulares
   c) encargados
   d) sujetos obligados

9. **Etapas de un plan de respuesta a incidentes de seguridad de datos personales.**

   a) Preparación, identificación, contención, mitigación, recuperación y mejora continua.
   b) Preparación, identificación, eliminación, mitigación, recuperación y mejora continua.
   c) Actuación, identificación, eliminación, mitigación, recuperación y mejora continua.
   d) Análisis, identificación, eliminación, mitigación, recuperación y mejora continua.

10. **El ____es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso no autorizado e ilegal de datos personales.**

    a) fraude
    b) robo de identidad
    c) phishing
    d) spamming