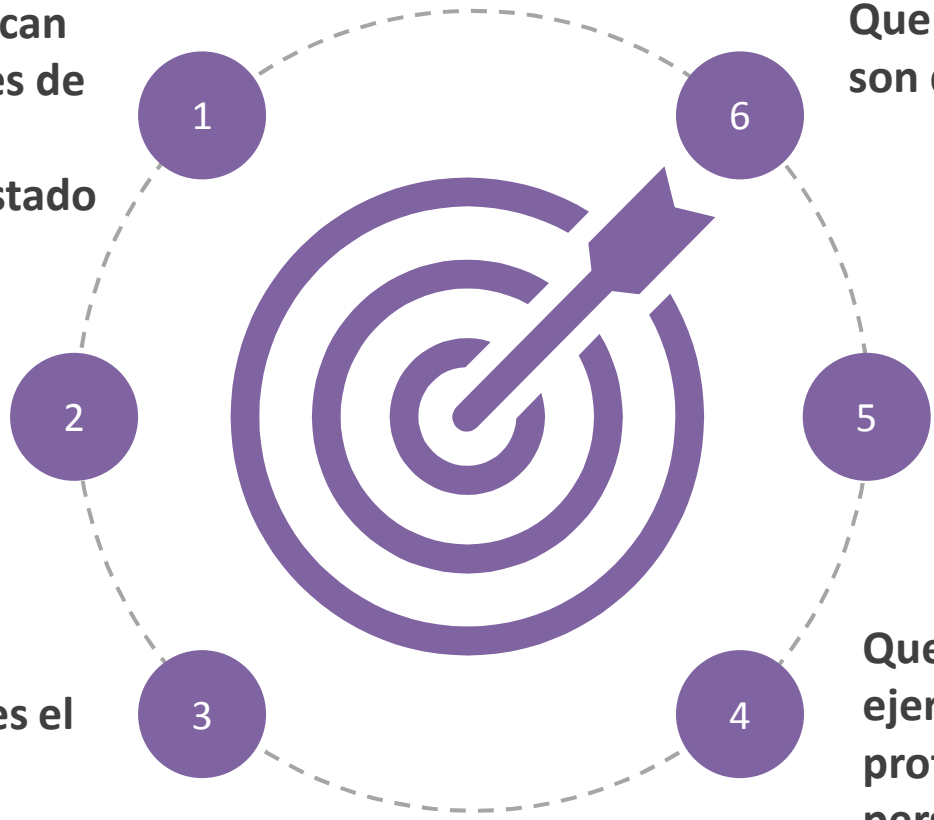
La Protección de tus Datos Personales

Objetivo General de la Plática

Dar a conocer a los alumnos información útil para el uso seguro y consciente de sus datos personales, así como para el ejercicio de su derecho.

Objetivos específicos

1. Que los alumnos conozcan aspectos fundamentales de la Ley de Protección de Datos Personales del Estado de Chihuahua.
2. Que sepan cuáles son los derechos ARCO.
3. Que conozcan qué es el Ichitaip.
4. Que sean capaces de ejercer su derecho de protección de datos personales.
5. Que reconozcan los datos personales de los estudiantes.
6. Que identifiquen cuáles son datos personales.



Generalidades de la Ley de PDP del Estado de Chihuahua

(Art. 1 LPDPCH)

La presente Ley es de orden público, interés social y de observancia general en el Estado de Chihuahua y tiene por objeto establecer las bases, principios y procedimientos, para garantizar el derecho que tiene toda persona a la protección de datos personales en posesión de los sujetos obligados.

Objeto de la Ley

(Art. 5 LPDPCH)

Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales.

Proveer los necesario para garantizar el ejercicio de los derechos ARCO.

Promover el establecimiento de medidas de seguridad.

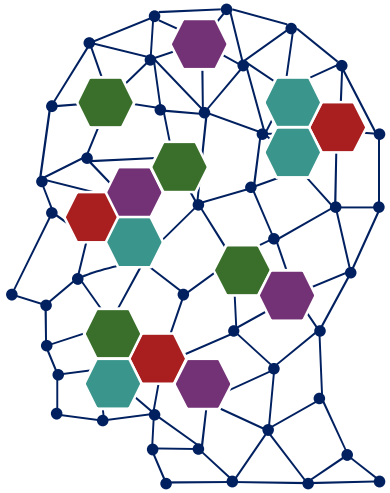
Establecer los mecanismos para garantizar el cumplimiento y la aplicación de las medidas de apremio.

Disposiciones Generales

¿Qué son los Datos Personales?

(Art. 11 Frac. VIII LPDPCH)

Cualquier información que se manifieste en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica, o en cualquier otro formato, concerniente a una persona física identificada o identificable, es decir, que pueda determinarse directa o indirectamente a través de cualquier información.



Los Datos Personales son irrenunciables, intransferibles e indelegables.

Datos personales sensibles

(Art. 11 Frac. IX LPDPCH)

Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Categorías

(Art. 11 Frac. VIII y IX LPDPCH)

- **Identificativos**
- **Electrónicos**
- **Laborales**
- **Patrimoniales**
- **Procedimientos administrativos y/o jurisdiccionales**

- **Académicos**
- Datos de tránsito y movimientos migratorios
- **Sobre la salud**
- **Biométricos**
- **Afectivos y familiares**

Sujetos Obligados

(Art. 6 LPDPCH)

- Ejecutivo
- Legislativo
- Judicial

- Órganos autónomos.
- Partidos políticos.
- Organismos descentralizados y desconcentrados de la administración pública estatal y municipal.
- Fideicomisos y fondos públicos.

- Ayuntamientos.
- Administraciones municipales.

Figuras

(Art. 11 y 28 LPDPCH)

Responsable

Sujeto Obligado

Titular

Dueño de los datos

Encargado

Persona ajena al SO que trata sus datos

Oficial

Protege los datos personales

Organismo Garante

Principios para el tratamiento de Datos Personales

(Art. 16 LPDPCH)

Consentimiento

(Art. 18 LPDPCH)

Tácito

No se opone al aviso de privacidad.

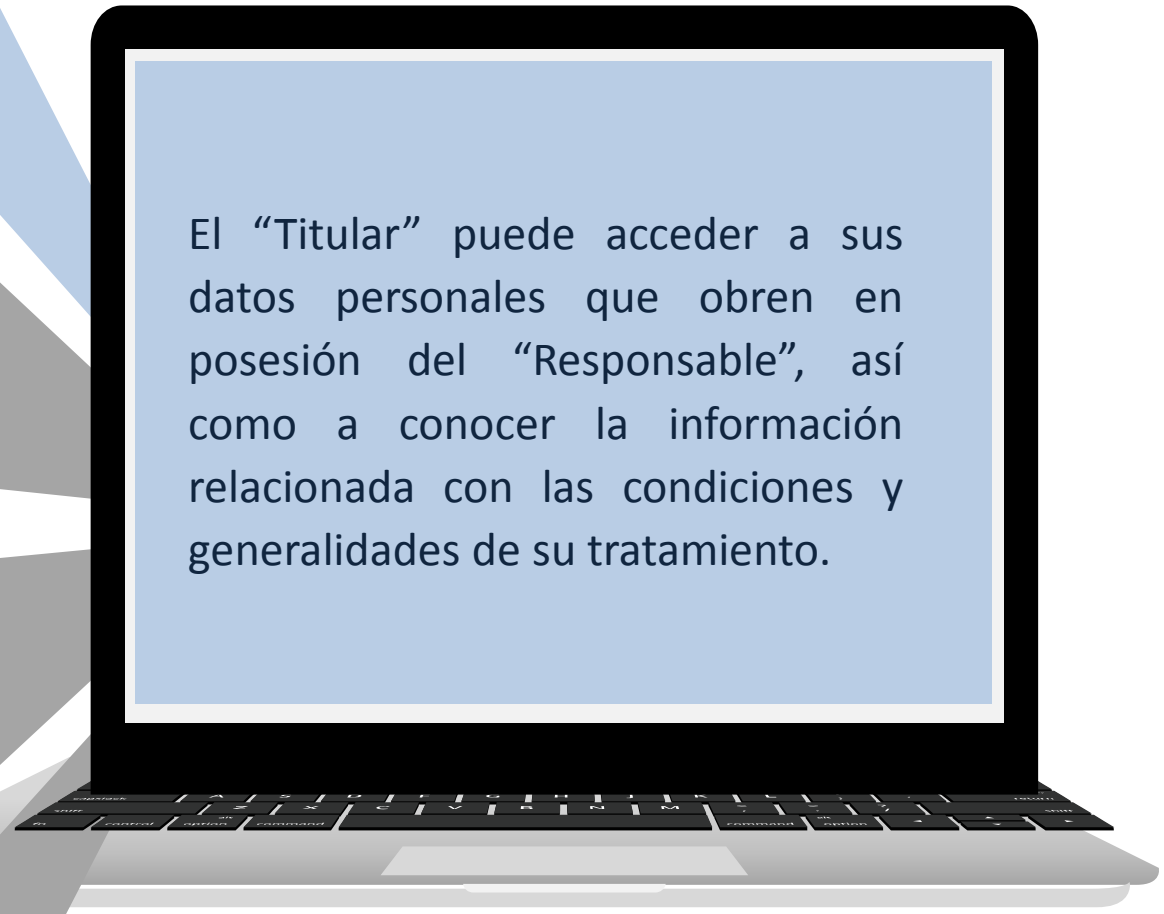
Expreso

Se manifiesta la voluntad verbalmente, por escrito, electrónico o signos inequívocos.

Trámite de derechos ARCO

(Art. 33 LPDPCH)

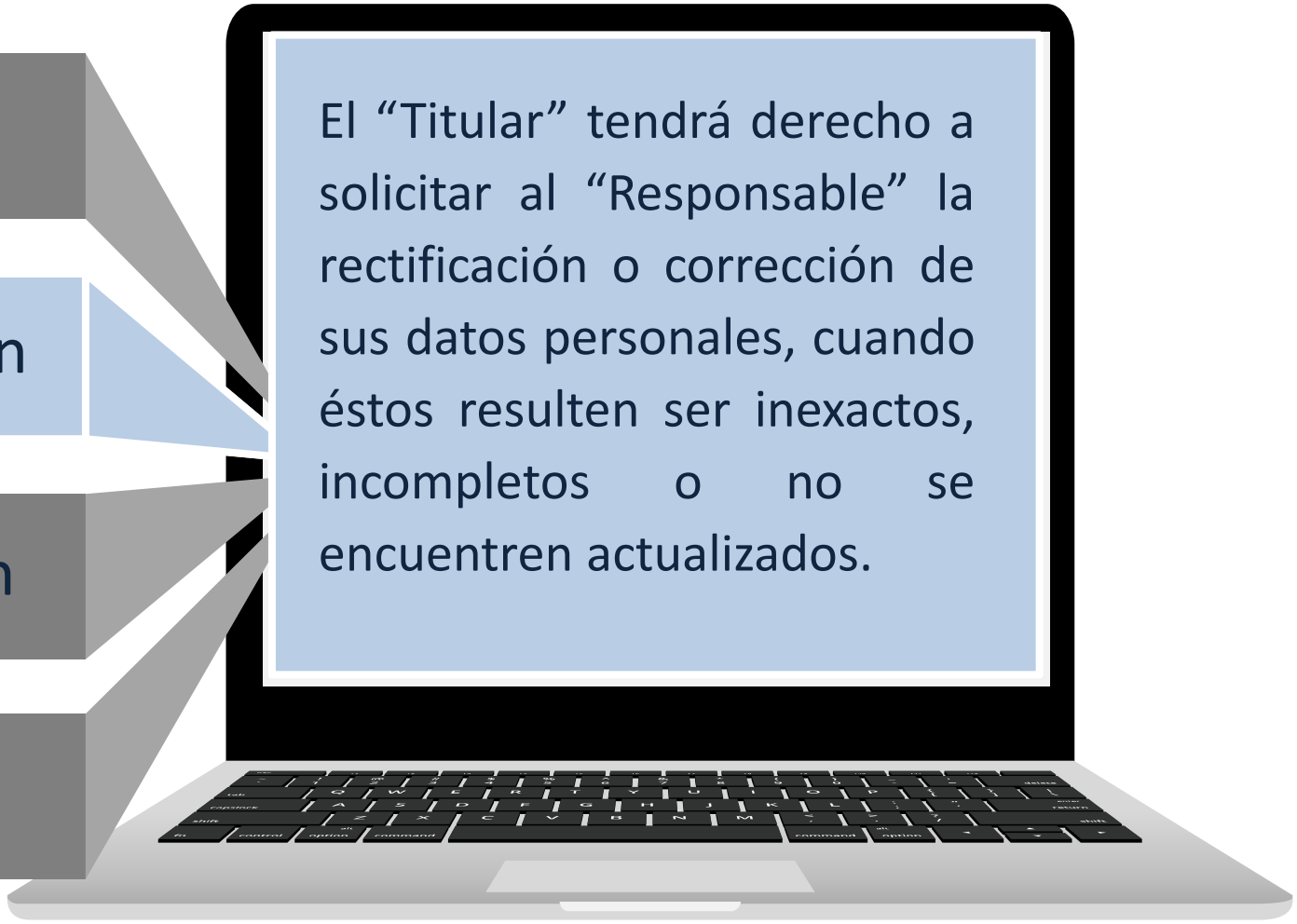
- Acceso
- Rectificación
- Cancelación
- Oposición



(Art. 34 LPDPCH)

- Acceso
- Rectificación
- Cancelación
- Oposición

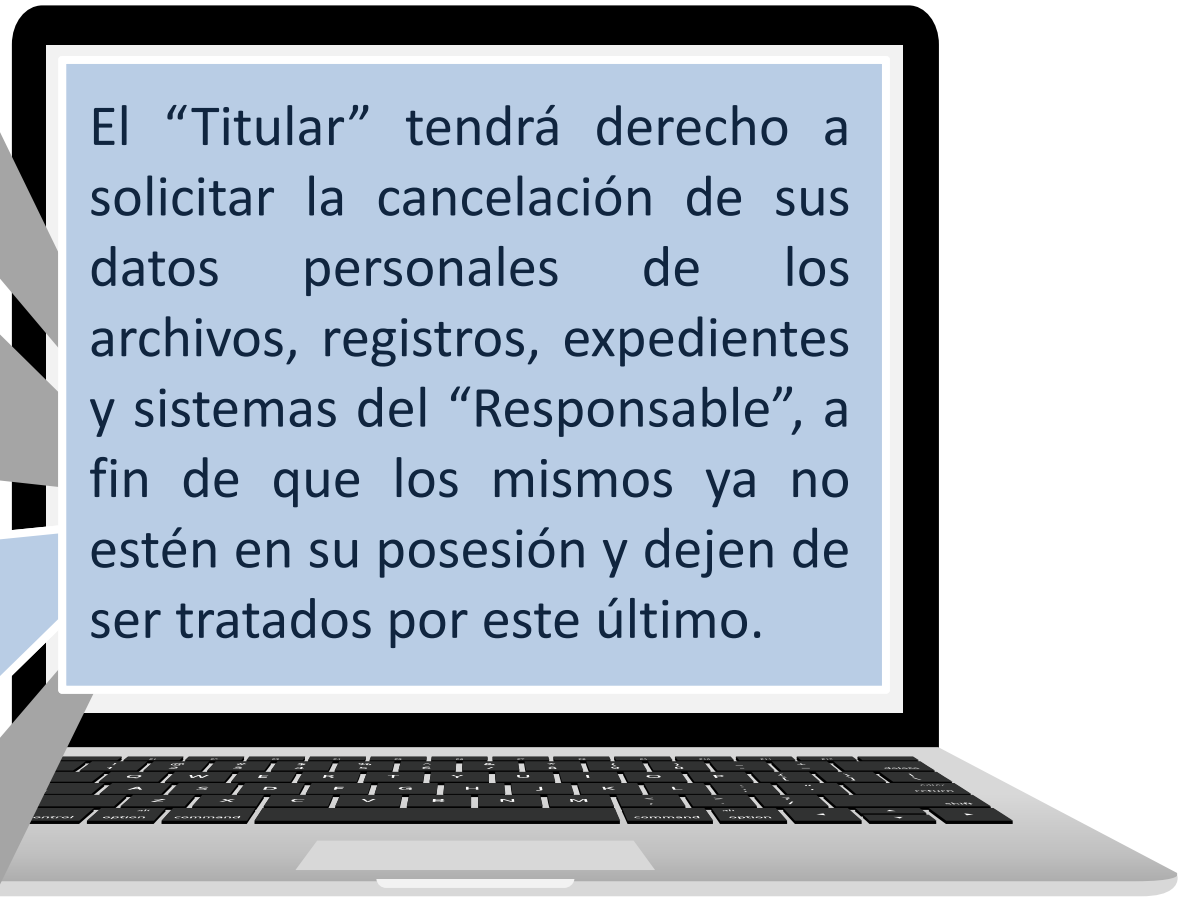
El “Titular” tendrá derecho a solicitar al “Responsable” la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.



(Art. 35 LPDPCH)

- Acceso
- Rectificación
- Cancelación
- Oposición

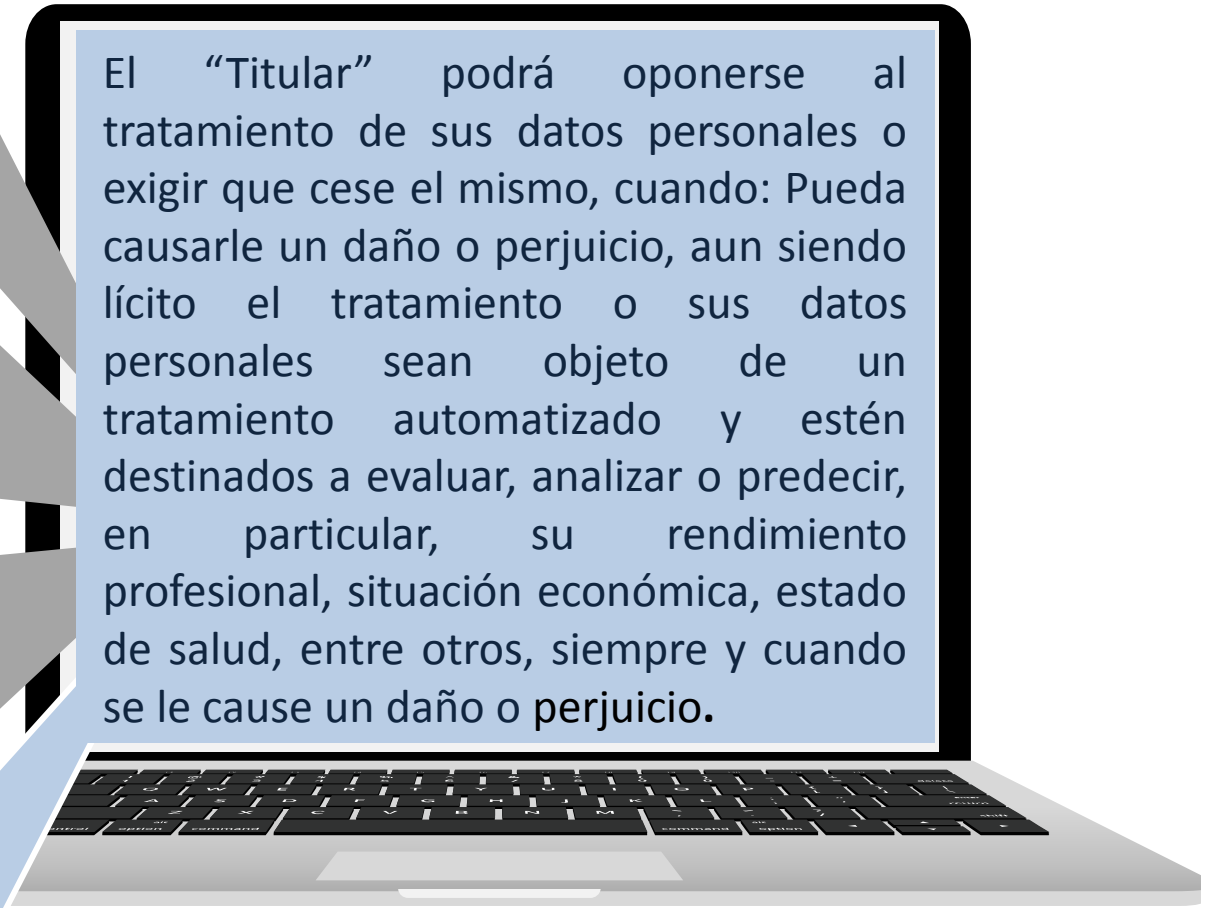
El “Titular” tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del “Responsable”, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.



(Art. 36 LPDPCH)

- Acceso
- Rectificación
- Cancelación
- Oposición

El “Titular” podrá oponerse al tratamiento de sus datos personales o exigir que cese el mismo, cuando: Pueda causarle un daño o perjuicio, aun siendo lícito el tratamiento o sus datos personales sean objeto de un tratamiento automatizado y estén destinados a evaluar, analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, entre otros, siempre y cuando se le cause un daño o perjuicio.



Portabilidad

(Art. 60 LPDPCH)

Es una modalidad del derecho de acceso para obtener una copia de sus datos personales en un formato electrónico.

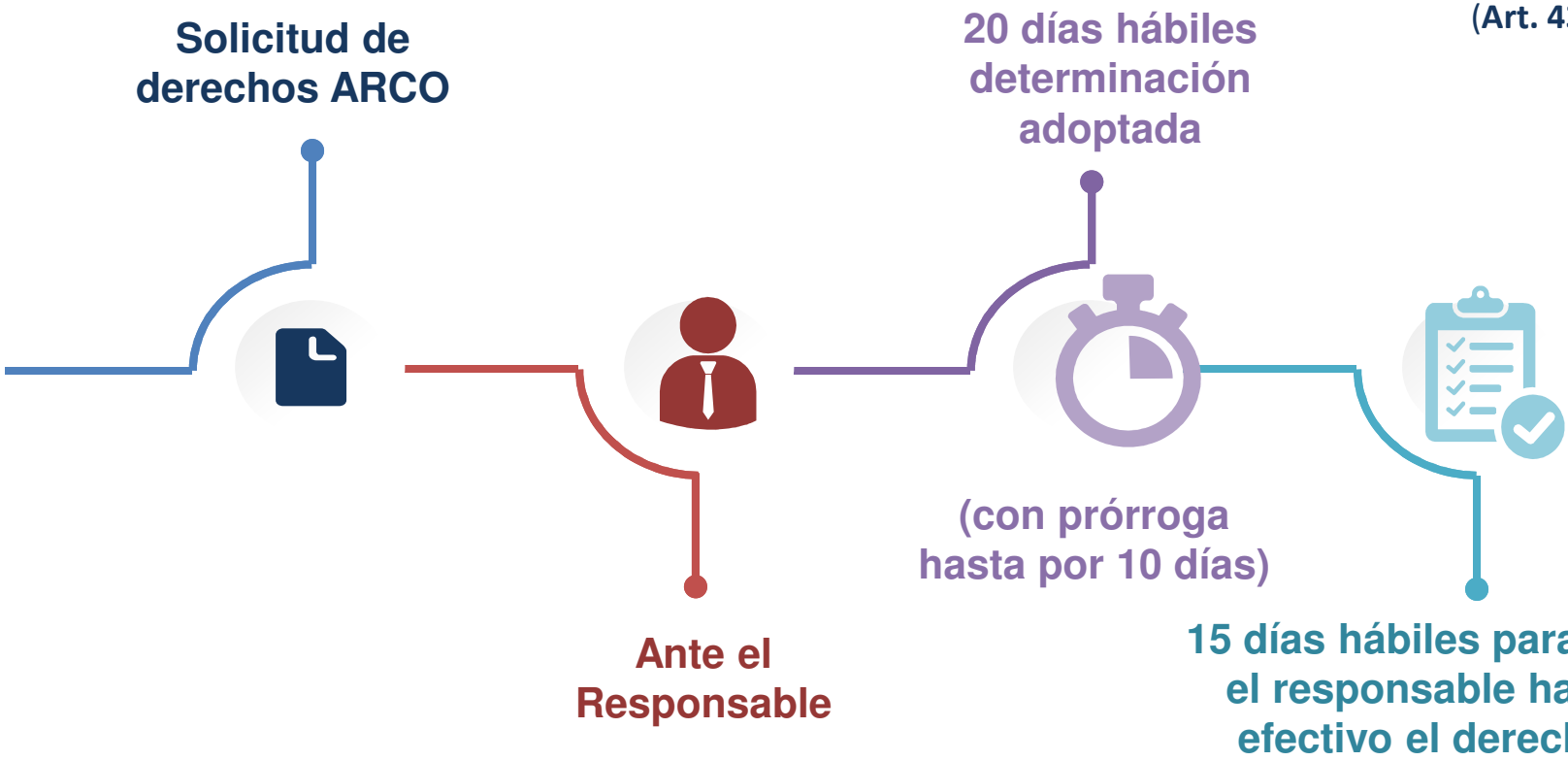
Transferencia

(Art. 11 Frac. XXXIV y 61 LPDPCH)

Transferir los datos personales de un sistema de tratamiento electrónico a otro. Debe estar en el aviso de privacidad.

Plazos para ejercer los derechos ARCO

(Art. 43 LPDPCH)

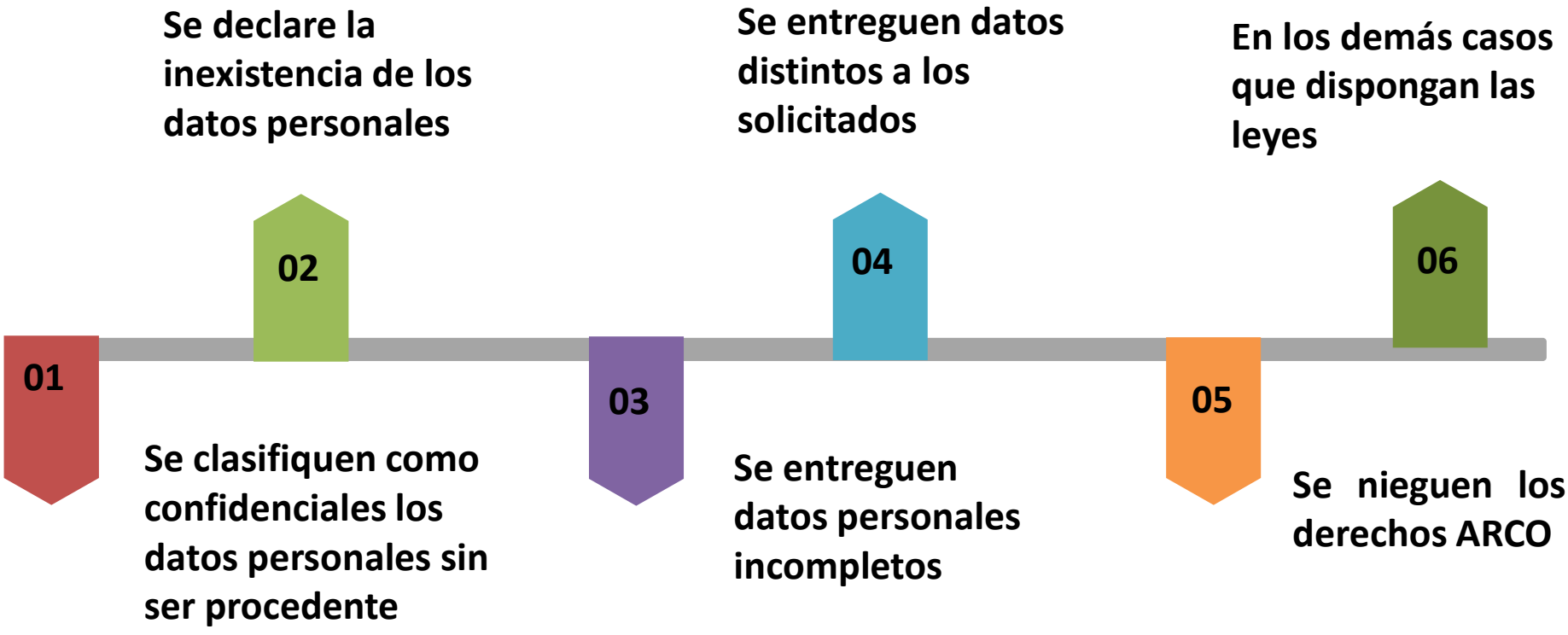


Recurso de Revisión

Sujetos Obligados

(Art. 111 LPDPCH)

Se interpone por el particular en la Unidad de Transparencia o ante el Instituto, y procede en casos de inconformidad del trámite de Derechos ARCO de SO. (15 días)



Procedimiento de Protección de Derechos

(Art. 45 LFPDP)

Particulares

- **Se iniciará a instancia del titular de los datos o de su representante legal.**
- **Redactar con claridad el contenido de su reclamación.**
- **La solicitud deberá presentarse ante el Instituto <u>15 días.</u>**

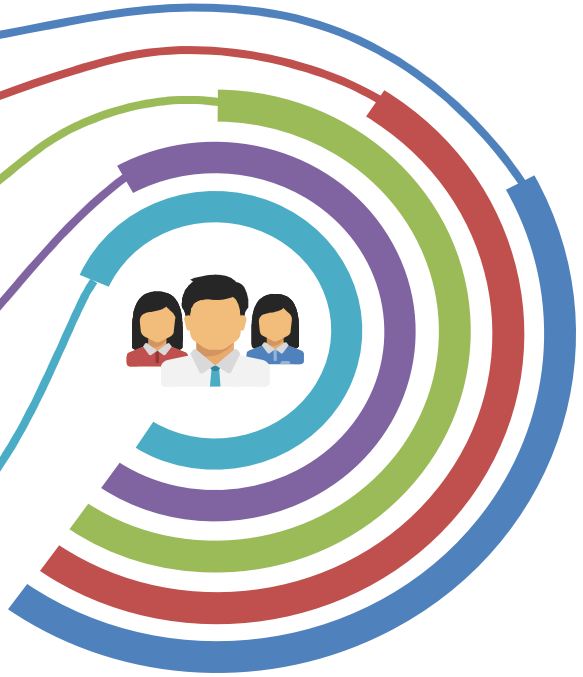
01 **Cuando el responsable no entregue al titular los datos personales solicitados**

02 **Lo haga en un formato incomprensible**

03 **Se niegue a efectuar modificaciones o correcciones a los datos personales**

04 **No corresponda a la información requerida**

05 **El titular no esté conforme con la información entregada por considerar que es incompleta**



Aviso de Privacidad

(Art. 11 y 66 LPDPCH)

AVISO DE PRIVACIDAD

Documento físico, electrónico o en cualquier otro formato que el responsable en el tratamiento de los datos personales pone a disposición del titular.

A través de éste, se le comunica al titular los datos personales que se recabarán y los fines para los cuales se hará.

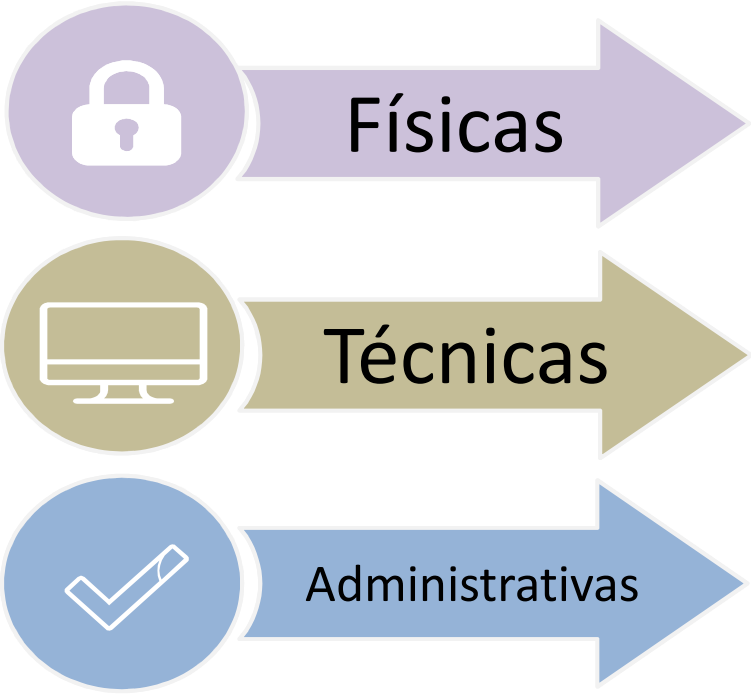
Debe contener identidad y domicilio de quien recaba los datos, opciones y medios para que los titulares limiten el uso o divulgación de los mismos.

También debe contener los medios para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición.

Medidas de seguridad

(Art. 73 LPDPCH)

El responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, así como garantizar su confidencialidad, integridad y disponibilidad.



Verificación

(Art. 142 y 143 LPDPCH)

El Organismo Garante deberá vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.

Podrá iniciarse de oficio cuando exista presunción de violaciones a la Ley o bien por denuncia ciudadana.

Ichitaip

(Art. 12 LTAIPCH y Art. 5 de la LPDPCH)

- Organismo público autónomo.
- Garantiza el derecho de acceso a la información pública.
- Protege los datos personales.
- Supervisa que los SO cumplan con la Ley.
- Aplica sanciones.
- Resuelve controversias.

- Pleno
- 5 Comisionados (as) Propietarios
- 5 Comisionados (as) Suplentes
- 7 años
- No podrán ser reelectos (as)

El Ichitaip debe:

(Art. 19 LTAIPCH)

I. Promover el derecho a la protección de datos personales, así como la cultura sobre su ejercicio y respeto.

II. Impulsar con instituciones de educación superior, la integración de centros de investigación, difusión y docencia sobre el derecho a la protección de datos personales.

III. Fomentar la creación de espacios de participación ciudadana.

El Ichitaip promueve el derecho

(Art. 19 LTAIPCH)

El Instituto, además de garantizar que la administración pública proteja los datos personales, es el responsable de promover y difundir el ejercicio de este derecho a través de pláticas a la sociedad en general:

- **Estudiantes.**
- **Docentes.**
- **Organizaciones de la sociedad civil.**
- **Empresarios.**
- **Colegios de profesionistas.**
- **Centros comunitarios, etc.**

Los datos personales y los jóvenes en la actualidad

Actualmente las nuevas generaciones utilizan sus datos personales de manera indistinta, lo que puede representar un riesgo para ser empleados con otros fines, por lo que es necesario tener conciencia del uso que se les da y tomar las medidas necesarias para prevenir una mala práctica de los mismos.

Datos personales de los alumnos

- Nombre
- Dirección
- Origen
- Calificaciones
- Matrícula
- Coeficiente intelectual
- Correo electrónico
- Situación financiera,

etc.

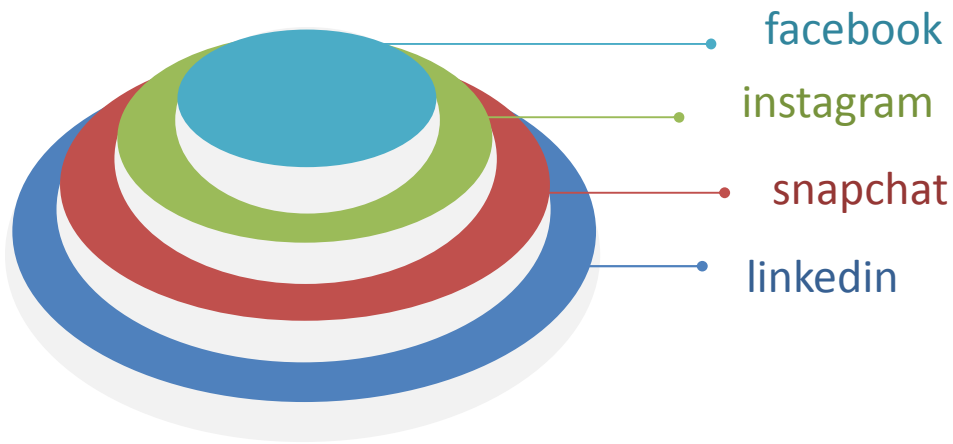
Redes Sociales/Internet

Más de 21 millones de niños y jóvenes de entre seis y 17 años de edad tienen acceso a Internet en México y pueden ser víctimas potenciales de delitos cibernéticos, por lo que es indispensable que comprendan la necesidad de proteger sus datos personales y tomen las medidas conducentes para evitar los malos manejos de sus datos.

Distribución

En México la red social más usada es facebook, mientras que instagram, snapchat o linkedin han aumentado su crecimiento en la red. Uno de cada 4 usuarios digitales mexicanos señala que permanece de entre una y dos horas diarias en redes sociales.

En América Latina, el tiempo promedio gastado semanalmente en redes sociales, es de 5.2 horas frente a 4 horas que se invierten en el e-mail.



El uso de las Redes Sociales

Para enterarse de rumores.

Para mantenerse al tanto de sus familiares y conocidos.

Para ver y compartir videos, chistes o cosas graciosas.

Para informarse de sucesos políticos o públicos.

Para compartir denuncias ciudadanas.

Para criticar el trabajo de las autoridades.

Riesgos

Actualmente las redes sociales se han convertido en las plataformas de difusión y comunicación entre usuarios más comunes, traspasando fronteras geográficas y creando comunidades con millones de internautas que comparten contenido. Evidentemente cada red social dispone de sus propias políticas de privacidad.

Se facilita información de carácter personal

Se almacena por la red social.

La red la comparte con empresas.

Muchas redes sociales, no utilizan un sistema de acceso y registro que pueda comprobar la identidad del usuario, lo cual puede ocasionar la creación de perfiles falsos con los riesgos para la integridad, intimidad y privacidad de los usuarios.

Ejemplos

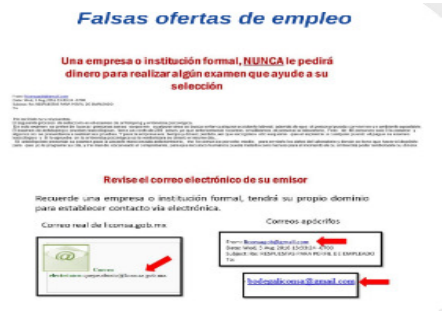
Fraude Banorte

Tiroteos en escuelas

Trata de personas

Ejemplos

Correos falsos de SHCP



Falsas ofertas de empleo

Página falsa de Ferromex

Agencia de viaje fraudulenta

Prevención

Consejos para proteger tus datos personales en Redes Sociales

Fuente :INAI

Evita intercambiar información personal y contraseñas a través de publicaciones y mensajes. *¡No las coloques en tu muro, timeline, ni por Messenger o mensaje directo!*

Ten mucho cuidado con la información que compartes en línea. *Evita mencionar dónde y con quién estás, o activa la confidencialidad de tus publicaciones para que solo puedan verlas tus contactos personales*

Lee detenidamente la política de privacidad de la red social en la sección: *"Términos y condiciones" antes de aceptar inscribirte en una red social*

Decide si tu perfil será público o restringido o privado en la parte de *"Configuración de la cuenta" o "Seguridad y privacidad de la cuenta"*

No reveles información personal en el contenido que compartes y evita colocarla en tu información de perfil. *Al revelar fotografías, domicilio, compras o lugares que frecuentas, te colocas a ti y a tus conocidos en riesgo*

Prevención

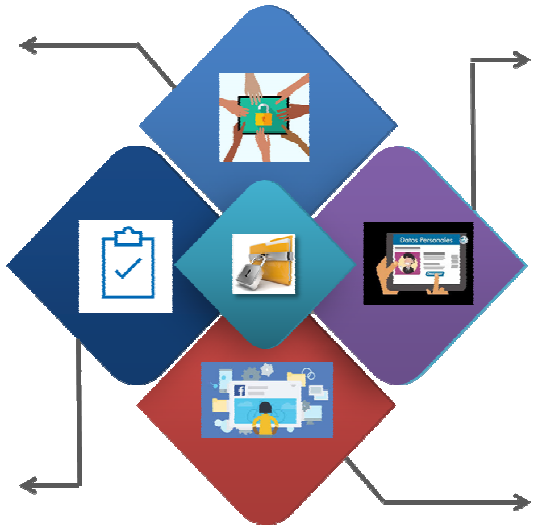
Fuente :INAI

Consejos para proteger tus datos personales en Redes Sociales

No reveles información personal en el contenido que compartes y evita colocarla en tu información de perfil.

Sé responsable en la Web: no tengas identidades falsas.

Descarga música, películas y software de manera legal.



Rechaza a cualquier desconocida/o que intente contactarte.

Aprende a bloquear contenidos o contactos no deseados.

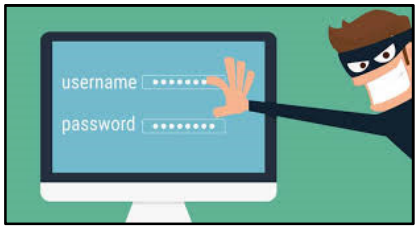
Asegúrate de que estás enviando tu información a las direcciones correctas.

Recomendaciones en Facebook

Fuente :El Economista

Cosas que podrías plantearte eliminar de tu Facebook:

- ✓ Cumpleaños
- ✓ Número de teléfono
- ✓ Algunos de tus “amigos”
- ✓ Las fotos de niños pequeños
- ✓ Información sobre las escuelas a las que van los menores (hijos, hermanos, etc)
- ✓ Servicios de localización
- ✓ Quejas sobre tu jefe o de la empresa donde trabajas
- ✓ Omite etiquetar tu localización
- ✓ Cuándo y dónde estás de vacaciones
- ✓ Los detalles de tu tarjeta de crédito
- ✓ Fotos de las tarjetas de embarque de los vuelos

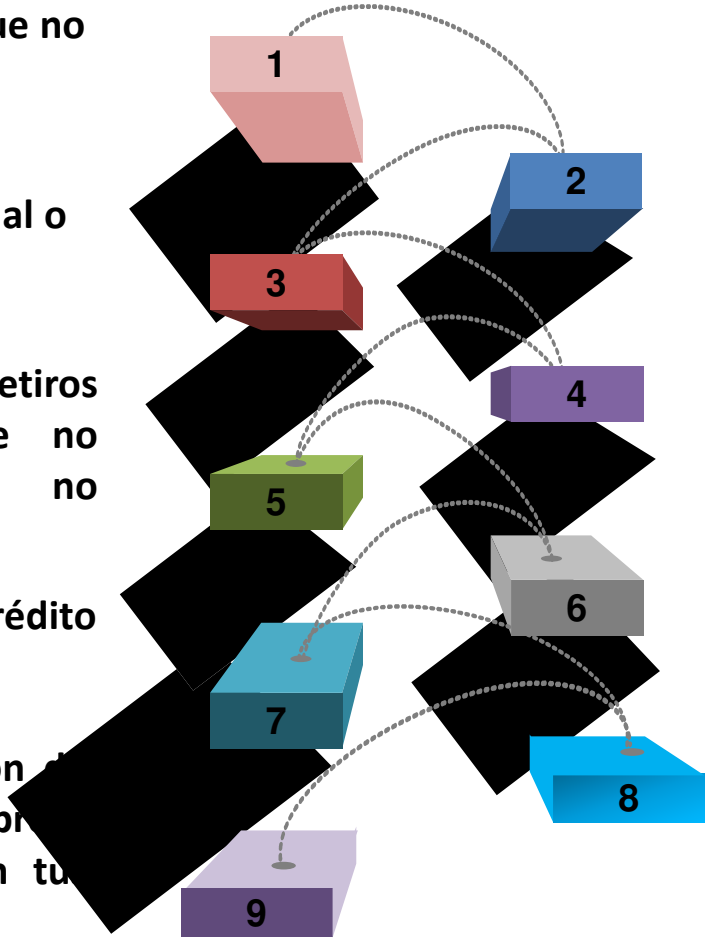


Robo de Identidad

Fuente: INAI

¿Cómo saber si has sido víctima de robo de identidad?

- ✓ Llamadas de despachos de cobranza por deudas que no adquiriste.
- ✓ Si dejas de recibir tu correspondencia habitual o se reduce considerablemente.
- ✓ Si observas cargos o retiros en tus tarjetas que no reconoces o que no realizaste.
- ✓ Recibir tarjetas de crédito que no solicitaste.
- ✓ Si recibes la notificación d vulneración de una empr que tiene en posesión tu datos personales.



- ✓ Encontrar diversos perfiles o usuarios que utilizan tu información y datos para hacerse pasar por ti.
- ✓ Si al utilizar tus tarjetas éstas son rechazadas.
- ✓ Cuando tus contactos reciben mensajes, correos electrónicos o llamadas a tu nombre y que tú no realizaste.
- ✓ Cuando descubres que contenido con tu información es publicado en perfiles o sitios que no son tuyos, sin tu autorización.

Prevención en robo de identidad

Fuente: INAI

01 Si haces pagos con tarjeta en línea evita usar redes públicas o gratuitas

02 Evitar tener el dispositivo móvil sin seguridad

03 No descuidar la correspondencia

04 Sólo lleva contigo los documentos necesarios para minimizar el daño en caso de robo o extravío

05 No proporciones datos confidenciales vía telefónica.

06 Procura tener siempre a la vista tu tarjeta de crédito o débito

07 Realiza transacciones seguras.

Robo de Identidad

Fuente: INAI

Plan de acción en caso de robo de identidad

1. Presenta tu denuncia ante las autoridades penales	Acude ante la Fiscalía General del Estado de Chihuahua y Procuraduría General de la República
2. Reportar la pérdida de los documentos a quién corresponda	Ante las instituciones bancarias si perdiste tus tarjetas de crédito o débito, ante la compañía de servicio telefónico
3. Cancela cuentas o servicios no autorizados que hayan sido contratados a tu nombre	Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) Procuraduría Federal del Consumidor (PROFECO)
4. Solicita una copia de tu reporte De crédito de forma gratuita ante el Buró de Crédito	Con tu reporte de crédito podrás conocer tu historial crediticio e identificar los créditos que hayas contratado, incluyendo aquellos que no reconozca

Robo de Identidad

Plan de acción en caso de robo de identidad

Fuente: INAI

5. Reportar en redes sociales el robo de identidad	**Informa a tus amigos, contactos y familiares que fuiste víctima de este delito para advertirles sobre actividad sospechosa que puedan realizar a tu nombre sin tu consentimiento, como solicitar datos personales o préstamos de dinero**
6. Contacta al INAI para reportar el uso indebido de DP	**El INAI no investiga de manera directa el robo de identidad ya que es atribución de las autoridades penales estatales, sin embargo, puede investigar el indebido tratamiento de tus datos personales**

Robo de Identidad Credencial

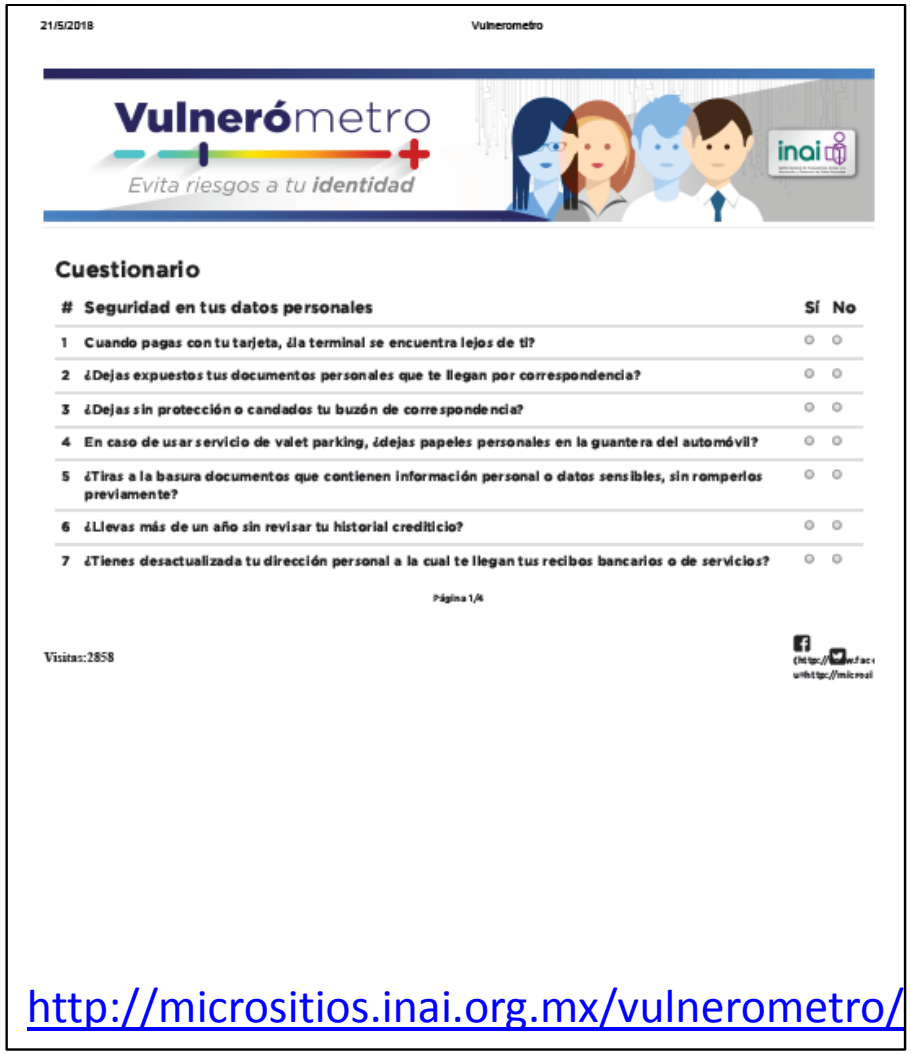
Fuente: INAI/Arestegui noticias

El mal uso de la información de este documento podría ser un riesgo para los titulares, como el **robo de identidad,** ya que contiene **datos personales** como: nombre completo, sexo, fecha de nacimiento, en algunos casos domicilio, entidad federativa, municipio y localidad, firma, fotografía, huella dactilar, Clave Única de Registro de Población (CURP) y clave de elector.

1. Solicitar la credencial para votar sólo cuando sea necesario.
2. Evitar conservar copias de la credencial para votar si no es necesario.
3. Resguardar las fotocopias o reproducciones de la credencial para votar con medidas de seguridad y confidencialidad adecuadas.
4. Eliminar los archivos o bases de datos que contengan la credencial para votar cuando hayan cumplido la finalidad para la cual fueron solicitados.
5. Medir el riesgo: entre más datos personales trates más obligaciones tendrás que cumplir.

Vulnerómetro

Fuente: INAI



21/5/2018 Vulnerometro

Vulnerómetro

Evita riesgos a tu identidad

inai

Cuestionario

#	Seguridad en tus datos personales	Sí	No
1	Cuando pagas con tu tarjeta, ¿la terminal se encuentra lejos de ti?	○	○
2	¿Dejas expuestos tus documentos personales que te llegan por correspondencia?	○	○
3	¿Dejas sin protección o candados tu buzón de correspondencia?	○	○
4	En caso de usar servicio de valet parking, ¿dejas papeles personales en la guantera del automóvil?	○	○
5	¿Tiras a la basura documentos que contienen información personal o datos sensibles, sin romperlos previamente?	○	○
6	¿Llevas más de un año sin revisar tu historial crediticio?	○	○
7	¿Tienes desactualizada tu dirección personal a la cual te llegan tus recibos bancarios o de servicios?	○	○

Página 1/4

Visitas:2858

http://micrositios.inai.org.mx/vulnerometro/

21/5/2018 Termometro

Vulnerómetro

Evita riesgos a tu identidad

inai

Respuestas: 19 (Sí) / 9 (No)

2 4 6 8 10 12 14 16 18 20 22 24 26 28

POCO VULNERABLE MUY VULNERABLE

Rango de Vulnerabilidad

RANGO 15-21

Mucho

Toma conciencia de tus hábitos ya que tus datos personales están en riesgo y sin control alguno, mejora el cuidado de tu información teniendo presente que alguien podría causar daño a tu reputación, tu persona o economía.

Entre más respuestas afirmativas tengas, más vulnerable eres de convertirte en víctima de robo de identidad

Te invitamos a consultar la Guía para prevenir el robo de identidad: Aquí

Regresar

Visitas:2859

Nuevas disposiciones

Fuente: El Universal/El Economista

El **Reglamento General de Protección de Datos de la Unión Europea** (GDPR por sus siglas en ingles) es una norma jurídica para "proteger a las personas físicas en lo que respecta al tratamiento de sus datos personales y la libre circulación de dichos datos" que entró en vigor el **25 de mayo de 2018**. Esta disposición tiene implicaciones en todo el mundo para empresas que fueron constituidas y operan en territorio europeo.

Pasos clave para cumplir con el Reglamento

Lo que necesitas saber sobre Avisos de Privacidad en Internet

Fuente: NYT

Datos biométricos

Fuente: INAI

Son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles, en mayor o menor medida:

Universales

Ya que son datos con los que contamos todas las personas.

Permanentes

Ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona.

Únicos

Ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas.

Medibles

De forma cuantitativa.

Características biométricas más comunes

Fuente: INAI

Huella dactilar. Se analiza el patrón global seguido por la huella dactilar.

Reconocimiento facial. Se analiza por la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.

Reconocimiento de iris. Una cámara infrarroja escanea el iris y proporciona sus detalles.

Geometría de la mano. Se extraen características que incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano.

Reconocimiento de retina. Se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma.

Reconocimiento vascular. Se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo.

El Ichitaip trabaja para apoyarte en la construcción de una nueva cultura de protección de datos personales para tu seguridad.

Técnicas para el robo de identidad y medidas preventivas

Fuente: INAI

Ingeniería social: a través de la interacción social, la manipulación y el engaño, usualmente a través de conversaciones directas.

- ✓ Solo carga aquellos documentos personales que vayas a utilizar.
- ✓ Ten copias de los mismos en algún lugar seguro de tu hogar (te serán de utilidad en caso de pérdida de los mismos) y, en caso de ya no ser necesarios, destrúyelos.

Extorsión telefónica: el atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como el empleado de alguna empresa o para verificar datos o actividades.

- ✓ Evita proporcionar información personal por vía telefónica a menos de que hayas escuchado el aviso de privacidad para conocer el tratamiento que se hará de tu información.
- ✓ Haz caso omiso de mensajes o llamadas que te comuniquen haber ganado un premio o que te hagan una oferta especial.

Observación: consiste en que el atacante pone atención a las acciones que realiza la víctima, utilizando algunas técnicas y herramientas de espionaje.

- ✓ No dejes tus documentos personales ni contraseñas en lugares públicos ni en tu automóvil a la vista de los demás.

Técnicas para el robo de identidad y medidas preventivas

Fuente: INAI

Dumpster diving: es a través de la búsqueda de información valiosa en basureros y desechos en domicilios y empresas.	✓ Antes de tirar tus documentos a la basura, asegúrate de que no contengan información personal. ✓ Si tus documentos contienen información personal lleva a cabo un borrado seguro como te lo explicamos anteriormente.
Robo de correspondencia, particularmente en buzones sin seguridad.	✓ Protege tu correspondencia utilizando un buzón con llave y recogiéndola lo más pronto posible.
Skimming o clonación de tarjetas: el atacante realiza una copia de la tarjeta de la vícitma. Suele utilizarse en cajeros automáticos manipulados y en establecimientos irregulares que guardan la información de la tarjeta para imprimirla en un plástico nuevo.	✓ Guarda todos los comprobantes de tus operaciones realizadas con tu tarjeta, no los tires en los cajeros o establecimientos donde la utilizaste. ✓ También revisa que el cajero no esté manipulado o que no contenga dispositivos extraños. ✓ Al teclear tu NIP, procura que no haya personas a tu alrededor.

Técnicas para el robo de identidad y medidas preventivas

Fuente: INAI

Spam: el correo electrónico basura o no deseado que llega masivamente a nuestras cuentas de correo sin ser solicitado y que presenta contenido sospechoso o engañoso, usualmente, de tipo publicitario. El contenido puede dirigir a la víctima al llenado de formularios en línea, o a la descarga de software para el robo de información desde el equipo de la víctima.

- ✓ Evita utilizar computadoras públicas para acceder a tu información personal o a redes abiertas de Wi-Fi para navegar en sitios en los que necesites ingresar tus datos personales.
- ✓ En caso de tener que utilizar tus cuentas de correo electrónico o redes sociales, asegúrate de cerrarlas correctamente al finalizar tu sesión y borrar tu historial de navegación.
- ✓ **No** permitas el uso remoto de tu computadora.
- ✓ No des click en vínculos que descarguen archivos o abran ventanas emergentes. Tampoco descargues archivos adjuntos a correos electrónicos de desconocidos.

Spim: similar al spam, la víctima recibe mensajes instantáneos que simulan ser invitaciones para suscribirse a promociones o servicios falsos, los cuales redirigen a la/el usuaria/o hacia sitios web maliciosos.

- ✓ Evita las ventanas emergentes de los navegadores que te recomiendan recordar tus contraseñas.
- ✓ Asegúrate de cambiar tus claves y contraseñas con regularidad y procura utilizar contraseñas seguras (longitud amplia y caracteres especiales).
- ✓ **NO** compartas tus contraseñas con nadie.