¿Cómo cuido mis datos personales? y ¿Qué deberían hacer las empresas para protegerlos?

Miriam J. Padilla Espinosa

Directora de Seguridad de Datos

Personales del Sector Privado

INAI

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

¿Qué son los datos personales?

- Los datos personales son cualquier información relativa a una **persona física**, que la identifica o hace identificable.

- Es la información que nos describe, que nos da identidad, nos caracteriza y diferencia de otros individuos.

- Datos personales sensibles

Son datos personales que informan sobre los **aspectos más íntimos de las personas**, y cuyo mal uso pueda provocar discriminaciones o ponerles en grave riesgo, como por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

En ese sentido, estos **datos requieren de especial protección y cuidado**.

¿Cuáles son los datos personales?

Opiniones políticas y afiliación sindical

Identificación y contacto

Patrimoniales y financieros

Laborales

Académicos

Datos salud

Datos biométricos

Pasatiempos, entretenimientos

Datos genéticos

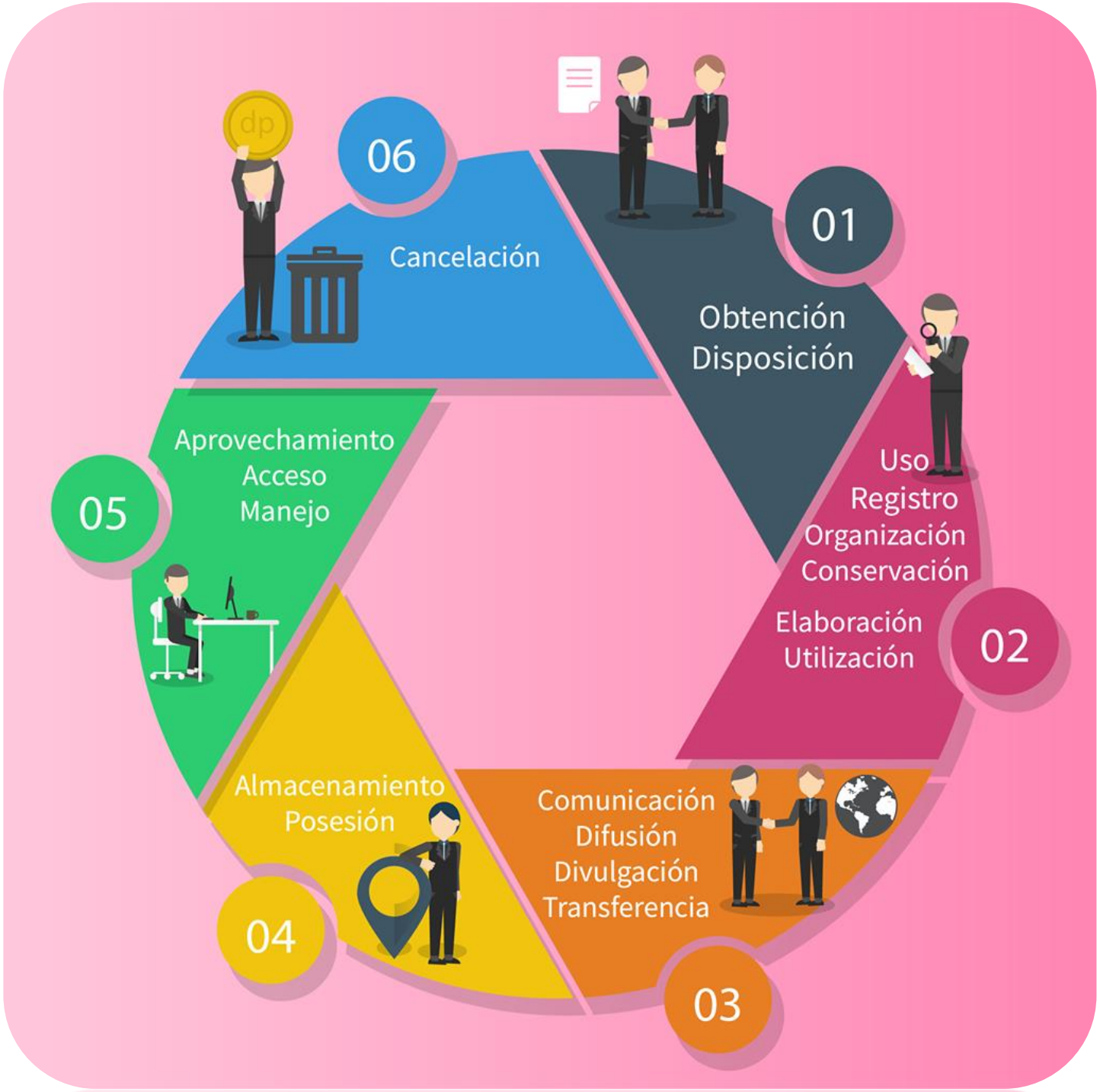
Datos jurídicos

Ideología, creencias filosóficas o morales

Características físicas

Datos migratorios

Datos de ubicación



DISC 2020

Tratamiento de datos personales

¿Quiénes tratan mis datos personales?

Particulares: Bancos, hospitales, hoteles, restaurantes, farmacias, escuelas, empresas de telefonía, internet, autoservicio, correo, personas físicas, entre otros.

Entidades públicas: Dependencias de gobierno federal, estatal y municipal, fiscalías, procuradurías, escuelas y hospitales públicos, oficinas de tránsito, centros de salud, entre otros.

Los datos personales tienen un valor…

Cuentas de juegos en Internet
12 a 3,500 US

Fotos y videos
desde 1 US

Enviar spam
70 a 150 US

Datos bancarios
desde 35.91 US

Cuenta de plataforma de pago online
desde 21.5 US

Historial de compra
20 US

Género
2.9 US

Passwords
76 US

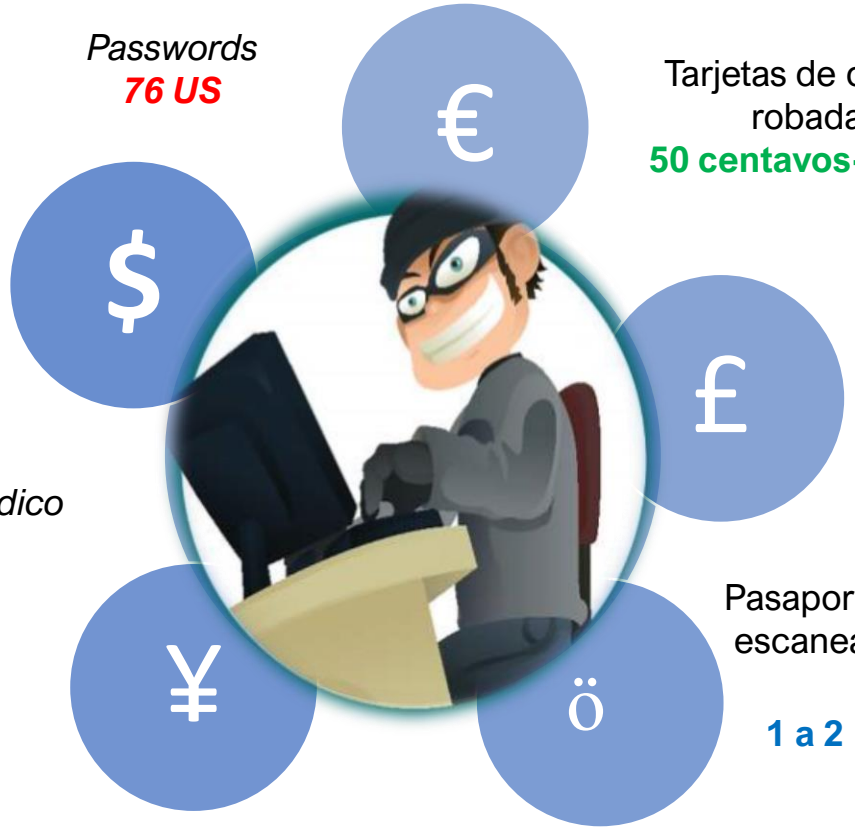
1,000 seguidores
2 a 12 US

Nombre
3.9 US

Registro médico
377 US

Historial de crédito
30 US

No. Teléfono
5.9 US



Tarjetas de crédito robadas
50 centavos- 20 US

Cuenta de redes sociales
desde 6 US

Pasaportes reales escaneados
1 a 2 US

Cuenta del correos electrónico
desde 5 US

Cuenta de servicios de pago multimedia
desde 12 US

Fuente:
Ponemon Institute, Privacy and Security in a Connected Life, Marzo 2015 http://goo.gl/C5pj89
¿Cuánto cuestan los datos robados y servicios de ataque en el mercado clandestino?
Symantec http://goo.gl/e41bec
https://www.osi.es/es/lo-que-han-pedido-los-ciberdelincuentes-los-reyes-magos

Riesgos en el tratamiento de datos personales

DISC 2020

- Exposición de datos personales.
- **Tratamiento desproporcional** de datos personales.
- **Vulneracion de datos personales**:
  - Pérdida o destrucción no autorizada.
  - Robo o extravío o copia no autorizada.
  - Uso, acceso o tratamiento no autorizado.
  - Daño alteración o modificación no autorizada.
- Incumplimiento al ejercicio de **derechos del interesado.**

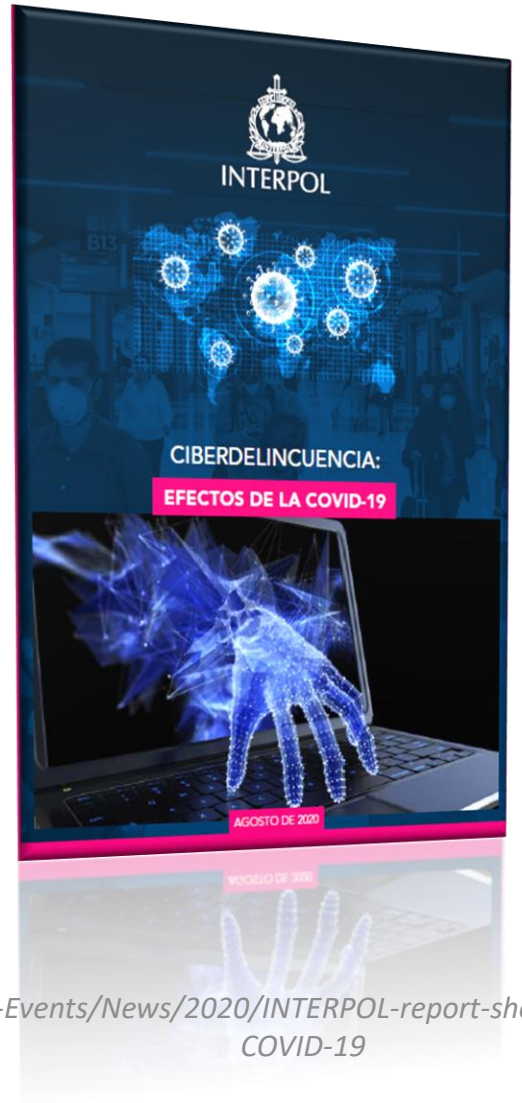
Nuevas amenazas …

Ransomware

Suplantación del CEO con el uso de deepfakes de audio

Ataque a dispositivos IoT

…que aprovechan el entorno



- **Las estafas por Internet y el phishing**
  Los autores de las amenazas han visto en la pandemia una oportunidad para aumentar las probabilidades de éxito de sus ataques y han aprovechado la ocasión para revisar sus sistemas habituales de estafas por Internet y phishing. Ahora envían a sus víctimas unos correos electrónicos de phishing sobre la COVID-19, a menudo haciéndose pasar por autoridades gubernamentales y sanitarias, en los que les incitan a facilitar sus datos personales y a descargarse contenidos maliciosos.
- **Los malwares disruptivos (ransomware y DDoS)**
  Alentados por la probabilidad de causar graves problemas y obtener sustanciosas ganancias, los ciberdelincuentes han multiplicado el número de ataques de malware disruptivos contra las infraestructuras esenciales y sanitarias. Los ataques de tipo ransomware o DDoS pueden provocar interrupciones frecuentes o la interrupción total de la actividad comercial, así como la pérdida temporal o permanente de información esencial.
- **Los malware de recolección de datos**
  En el ámbito de la ciberdelincuencia también están en auge los ataques de malware para recolectar datos, como los troyanos de acceso a distancia, los ladrones de información, los spyware (programas espía) o los troyanos bancarios, entre otros. Los autores de las amenazas utilizan información relacionada con la COVID-19 como señuelo para infiltrarse en los sistemas e infectar redes, sustraer datos, desviar fondos y crear botnets.
- **Dominios malignos**
  Se ha producido un aumento considerable del número de ciberdelincuentes que, aprovechando el incremento de la demanda de productos médicos e información sobre la COVID-19, registran nombres de dominio que contienen palabras clave relacionadas con la pandemia, como "coronavirus" o "COVID". Se trata de sitios web fraudulentos que esconden una amplia variedad de actividades malignas, por ejemplo, servidores C2, difusión de malware y phishing.
- **Desinformación**
  Asistimos a una amplificación de la desinformación y noticias falsas que se propagan rápidamente entre la población. Alimentadas por la incertidumbre de la situación socioeconómica en el mundo, la información no contrastada, las amenazas mal entendidas, y las teorías de la conspiración han fomentado la ansiedad de los ciudadanos y, en algunos casos, facilitado la ejecución de ciberataques.

Fuente:
https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

… con una mejor organización

… y con motivaciones específicas

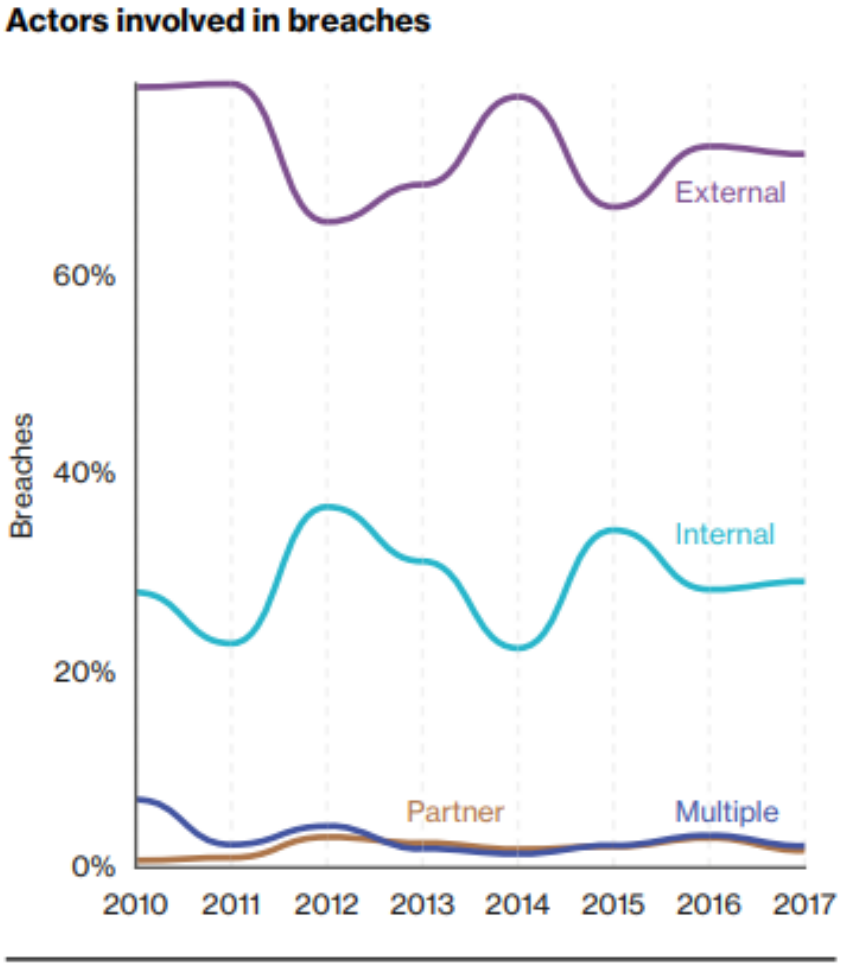


Figure 1. Threat actors within breaches over time

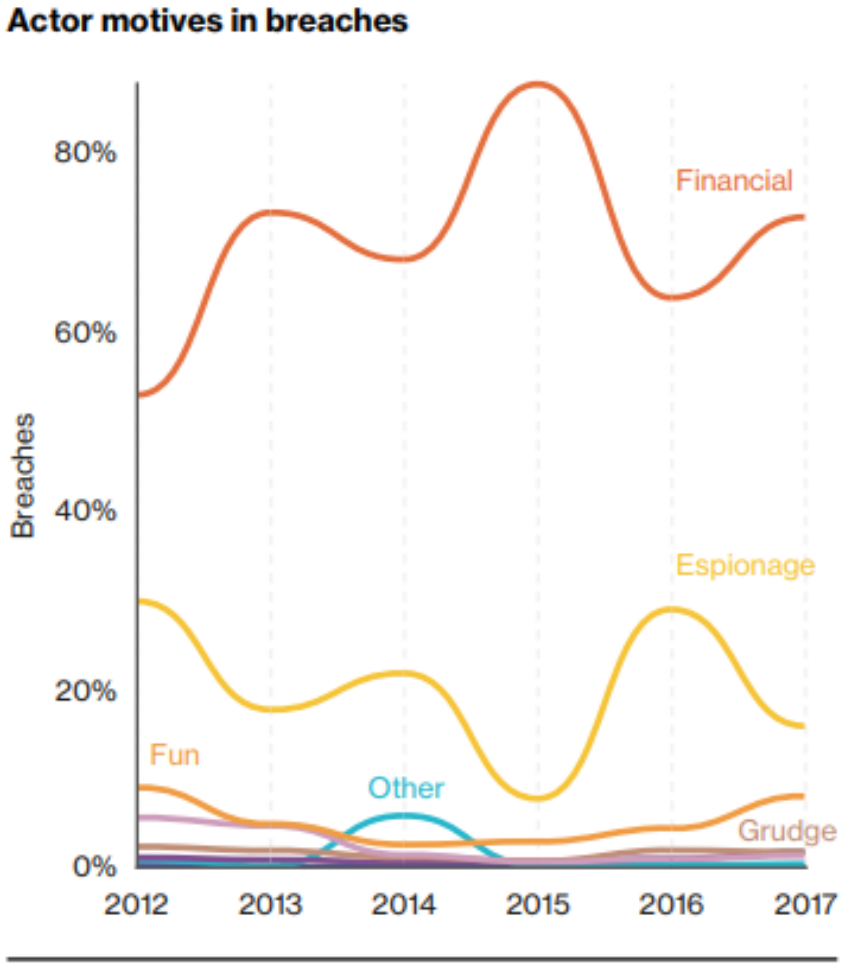


Figure 2. Threat actor motives within breaches over time

Fuente: Verizon 2018 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Tratamiento indebido de datos personales

- Tratar los datos personales en contraversión a los principios establecidos en la Ley
- No contar con un aviso de privacidad
- Que el aviso de privacidad omita algún elemento obligatorio
- Tener datos inexactos
- Hacer transferencias de datos a terceros sin comunicarles en el aviso de privacidad
- Incumplir el deber de confidencialidad
- Cambiar sustancialmente la finalidad originaria del tratamiento de los datos
- Realizar transferencias de datos sin el consentimiento expreso del titular, cuando este sea exigible
- Obtener datos de forma engañosa y fraudulenta
- Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO

Consecuencias de un tratamiento indebido de datos personales

- Pérdidas financieras
- Fraude
- Uso no autorizado de cuentas y/o datos personales
- Discriminación
- Daño a la reputación, al honor o la integridad física del titular

Marco legal en materia de PDP

DISC 2020

PRIVADO

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

- RLFPDPPP
- Lineamientos Aviso de Privacidad
- Lineamientos hiperenlaces e hipervínculos AP
- Criterios Generales instrumentación medidas compensatorias
- Parámetros de Autorregulación
- Reglas de Operación REA
- Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales
- Recomendaciones en materia de seguridad de datos personales
- Guía implementación SGDP
- Metodología de Análisis de Riesgo BAA
- Guía para cumplir con principios y deberes
- Guía para el borrado seguro de DP
- Manual para MiPyMEs
- Tabla de Equivalencia Funcional
- Recomendaciones designación responsable al interior
- Guía para Instrumentar Medidas Compensatorias
- El ABC del aviso de privacidad

- Guía para el tratamiento de datos biométricos
- Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales
- Recomendaciones para el manejo de incidentes de seguridad de datos personales

PÚBLICO

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Leyes estatales en materia de protección de datos personales

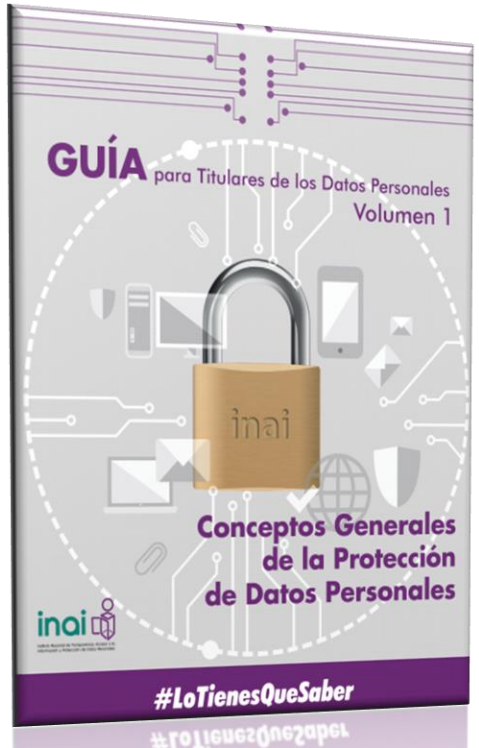
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Parámetros de **Mejores Prácticas** en Materia de Protección de Datos Personales del Sector Público
- Reglas de operación del Registro de **Esquemas de Mejores Prácticas**
- Lineamientos modalidades y procedimientos para la **portabilidad** de datos personales
- Disposiciones administrativas de carácter general para la elaboración, **presentación y valoración de evaluaciones de impacto en la protección de datos personales**.
- Criterios generales para la instrumentación de **medidas compensatorias en el sector público** del orden federal, estatal y municipal.
- Programa de Protección de Datos Personales
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- El ABC del aviso de privacidad (Sector Público)
- Guía para la elaboración del aviso de privacidad en el área de recursos humanos (Sector Público)

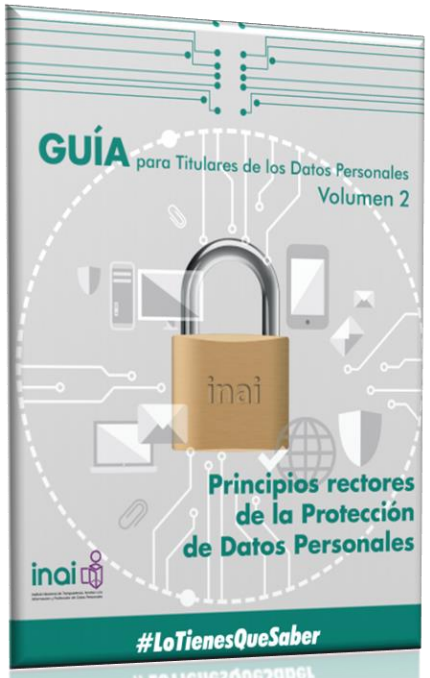
- Guía para el tratamiento de datos biométricos
- Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales
- Recomendaciones para el manejo de incidentes de seguridad de datos personales

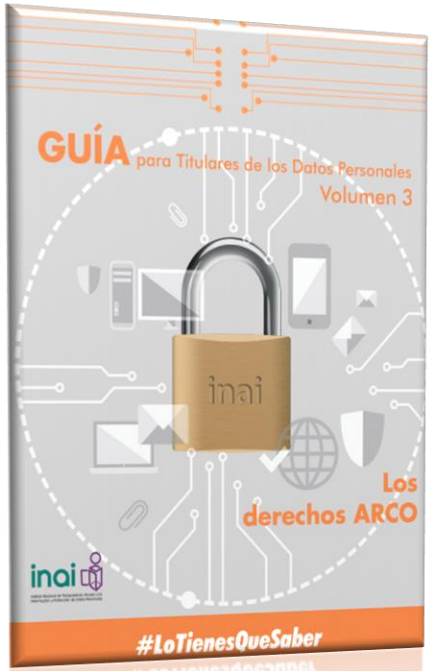
¿Cómo cuido mis datos personales?

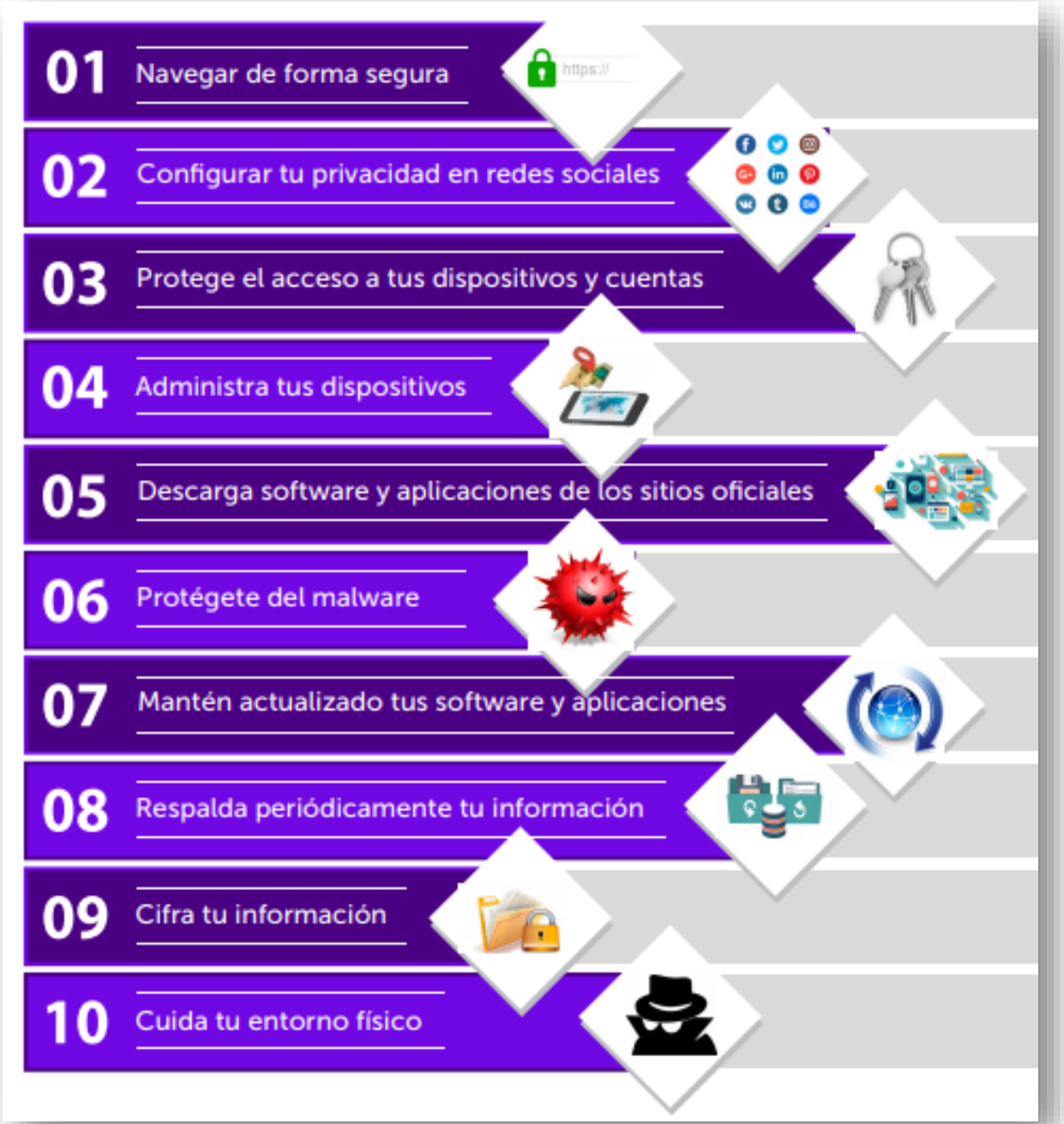
DISC
2020

Conocer y ejercer tu derecho a la protección de tus datos personales









DISC 2020

Recomendaciones para mantener seguridad tu privacidad y datos personales en el entorno digital

inai

#TusDatosValen

DISC 2020

¡PROTEGE TUS DATOS PERSONALES!

#TusDatosValen

INAImx INAImexico inai_mx inaimexico

A Evita proporcionar tus datos personales a través de llamadas telefónicas.

B Al navegar por Internet, verifica siempre que el sitio que solicita tus datos personales corresponda al sitio de la institución u organización que dice ser.

C Evita ingresar a sitios web a través de enlaces incluidos en correos electrónicos, mensajes de texto o publicados en redes sociales.

D Configura los filtros de correo no deseado y fraudulento en tu correo electrónico.

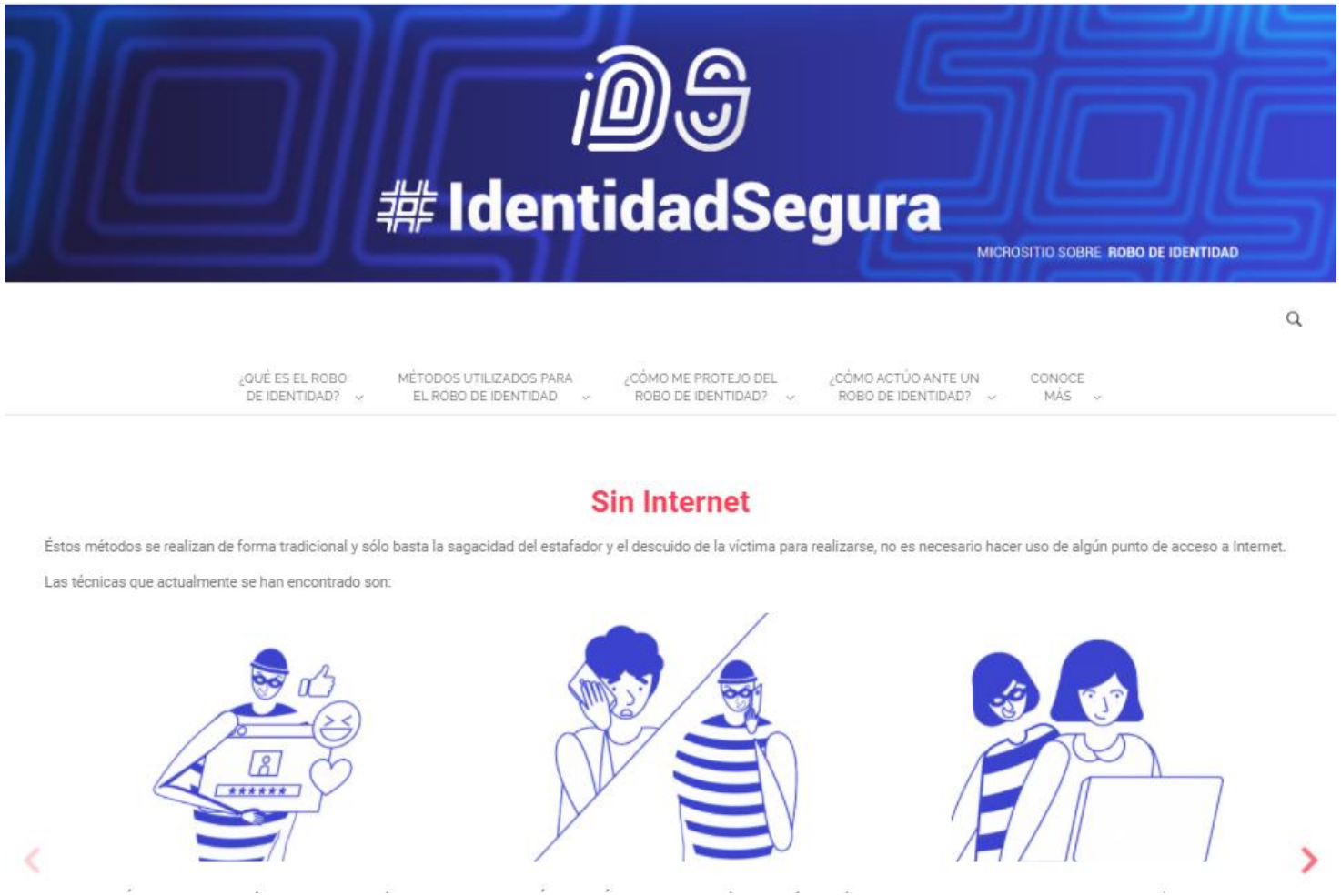
inai

Acércate al INAI

El **INAI** es la autoridad garante del derecho a la protección de datos personales, por lo tanto, podrás acudir ante esta autoridad cuando tengas conocimiento de un **tratamiento indebido de los datos personales**, y hacer uso de los procedimientos señalados en:

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), cuando resulten procedentes.

Micrositio #IdentidadSegura



https://micrositios.inai.org.mx/identidadsegura/
Micrositio sobre Robo de Identidad

Micrositio ¡clic!

https://micrositios.inai.org.mx/clic/
Niñas, niños y adolescentes

Infografías

¿Qué deberían hacer las empresas para protegerlos?

DISC
2020

Principios, deberes y obligaciones (capacitación)

DERECHOS

- Acceso
- Rectificación
- Cancelación
- Oposición

PRINCIPIOS

- Licitud
- Consentimiento
- Proporcionalidad
- Calidad
- Lealtad
- Información
- Finalidad
- Responsabilidad

DEBERES

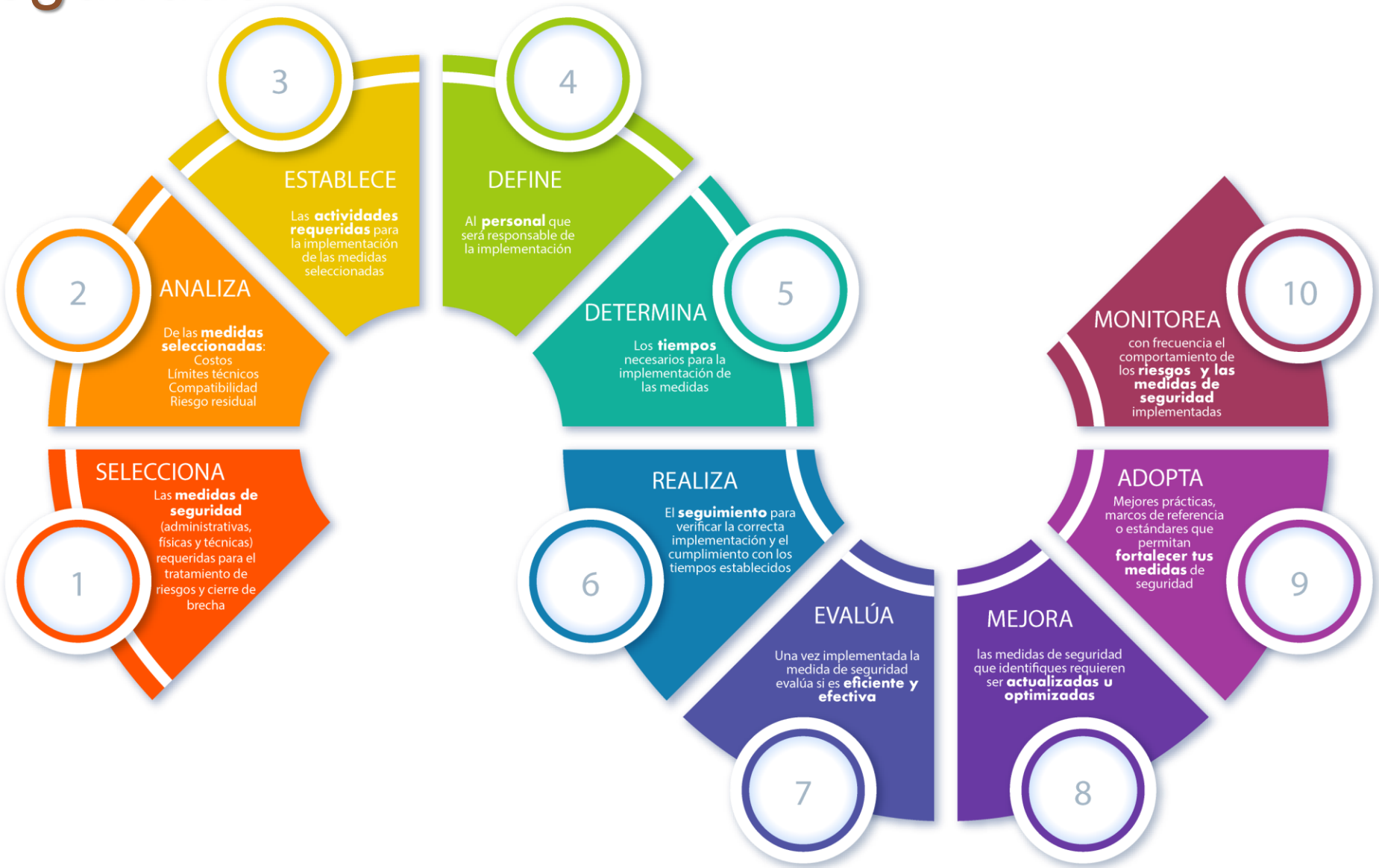
- Seguridad
- Confidencialidad

Guías y recomendaciones

Publicación de documentos, y otras referencias respecto al deber de seguridad

Actividades mínimas para la seguridad de los datos personales

Planeación de la implementación de las medidas de seguridad



- Claridad en los **tratamientos** que se realizan
- Atender **quejas o dudas.**
- Brindar mecanismos que **faciliten las solicitudes** de derechos ARCO.

Cercanía con los titulares

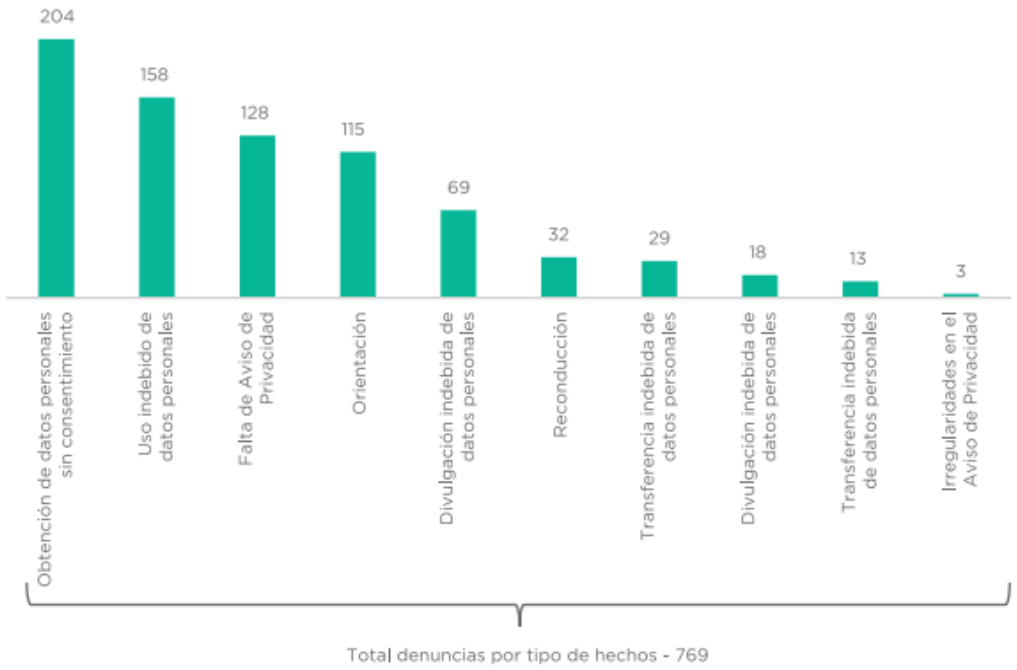
Fuente: Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales – INAI

DISC 2020

Gestión de vulneraciones a la seguridad de los datos personales

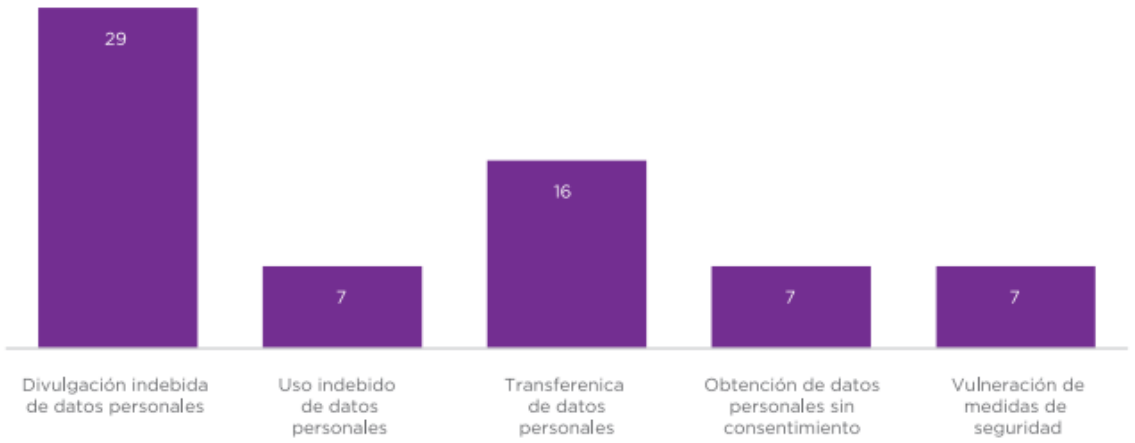
Aprender de los errores

GRÁFICA 7.14 Denuncias por tipo de hechos (sector privado)



FUENTE: INAI, Secretaría de Protección de Datos Personales, Dirección General de Investigación y Verificación del Sector Privado.

GRÁFICA 7.17 Clasificación de expedientes por tipo de hechos



FUENTE: INAI, Secretaría de Protección de Datos Personales, Dirección General de Evaluación, Investigación y Verificación del Sector Público.

Fuente: Informe de Labores 2019 INAI- http://inicio.inai.org.mx/Informes%202019/Informe_2019.pdf

Incorporar buenas prácticas

- **Sistema de Gestión de Datos Personales**.
  - Esquemas de Autorregulación
  - Esquemas de mejores prácticas
- **Demostrar cumplimiento** ante la autoridad

Registro de Esquemas de Autorregulación

Marca INAI

Registro de Esquemas de Autorregulación Vinculante

http://rea.inai.org.mx/

DISC 2020

Auditorías Voluntarias (Sector Público)

AUDITORÍAS VOLUNTARIAS
EN MATERIA DE **PROTECCIÓN** DE **DATOS PERSONALES**

Si eres **responsable del tratamiento de datos personales** a nivel federal, el **INAI** te orienta para que **fortalezcas el cumplimiento de tus obligaciones**

¿Cómo?

¡Solicita al INAI una auditoría voluntaria!

¿Qué es?

Es un **proceso sistemático**, independiente y documentado que **evalúa los controles, medidas y mecanismos** implementados por ti, **en el tratamiento de datos personales**

Beneficios

- Posibilita **determinar el grado de cumplimiento** de las disposiciones previstas en la **LGPDPPSO ***
- Permite **detectar posibles inconsistencias y prevenir sanciones**
- Contribuye a la **revisión, mantenimiento y mejora** del Sistema de Gestión de Seguridad de Datos Personales

**Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*

+ Información

55-50-04-24-00
Ext. 25-74

auditoriasvoluntarias@inai.org.mx

inai

@INAImx @INAImexico inai_mx inaimexico

#ElQuePreguntaNoSeEquivoca

Tel inai

Premio de Innovación y Buenas Prácticas en la PDP

LA PROTECCIÓN DE DATOS PERSONALES ES UNA RESPONABILIDAD COMPARTIDA

Gracias

Miriam J. Padilla Espinosa

Directora de Seguridad de Datos Personales del Sector Privado
INAI

miriam.padilla@inai.org.mx

@Ing_Mili