AMAI 25 AÑOS
INTELIGENCIA APLICADA A DECISIONES

Protección de Datos Personales

Manual de buenas prácticas

13 de abril 2017

Introducción

El presente documento tiene por objeto orientar a las agencias de Investigación de Mercados, en el cumplimiento de las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento, con relación a las medidas de seguridad para la protección de los datos personales, y para poder implementar algunas medidas de gestión que sugieren las Recomendaciones en materia de Seguridad de Datos Personales (Recomendaciones), publicadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el Diario Oficial de la Federación (DOF), el 30 de octubre de 2013.

LFPDPPP artículo 19, señala que **todo sujeto regulado que use datos personales debe establecer y mantener en el tiempo, controles de seguridad para proteger los datos que estén en su posesión.** Es decir, si sabemos dónde y cómo recabamos, almacenamos, utilizamos y eliminamos la información, entonces sabremos dónde necesitamos establecer medidas de seguridad.

Las razones para estar interesados en la protección de datos personales, implican que:

- Se trata de un derecho humano de los titulares y una obligación para quienes los utilizan.

Introducción

- Ayuda a prevenir y mitigar los efectos de una fuga y/o mal uso de los datos personales.
- Evita afectaciones económicas como consecuencia de multas, compensaciones de daños, pérdidas de clientes e inversionistas.
- Se mejoran los procesos de la organización y se incrementa el nivel de confianza entre las partes interesadas: clientes, inversionistas, empleados, colaboradores, pero sobre todo con los titulares.

Reglamento artículo 47, señala que **toda persona física o moral que trate datos personales tiene la obligación de velar por su resguardo y uso adecuado** (principio de responsabilidad). Para ello, se debe **comenzar por poner orden en los procesos** y documentar los procedimientos.

Acciones para la seguridad de los datos personales

Este es el Sistema de Gestión de Seguridad de Datos Personales propuesto por el INAI, el cual tiene por objeto el proponer un marco de trabajo para el tratamiento de los datos personales.

El sistema propuesto es compatible con las fases del ciclo de Planear, Hacer, Verificar y Actuar (PHVA), que también es la base para los Sistemas de Gestión de la Calidad (SGC).

Esto implicaría empatar el sistema existente, es decir, incorporar la Protección de Datos Personales a los procesos del negocio.

Fuente: Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, INAI, Junio 2015

Comercialización, diseño y propuesta de investigación

Al dar respuesta a una solicitud del cliente, considerar los siguientes aspectos relacionados con el tratamiento de los datos personales:

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

- Datos personales a recabar (de identificación, sensibles, patrimoniales, financieros), así como su método de recolección y supervisión.

Datos personales: cualquier información concerniente a una persona física identificada o identificable, que puede estar expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

Datos personales sensibles: refieren a información que pueda revelar aspectos íntimos de una persona o dar lugar a discriminación

Comercialización, diseño y propuesta de investigación

- Incorporar al contrato, si se fungirá como responsable o encargado.

- Notificar el empleo de proveedores.

Reglamento, Artículo 54.

“ Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último.

Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. ”

Comercialización, diseño y propuesta de investigación

- Si se recibe base de datos personales por parte del cliente, verificar que su aviso de privacidad (AP), considere la finalidad de investigación de mercados/ encuestas de satisfacción dentro de sus finalidades.
  - Formalizar la recepción de base de datos personales mediante oficio, especificando los datos personales que se reciben (éstos deben ser acordes a la finalidad del estudio).

- Incluir en las reuniones de discusión con los responsables del proyecto, el tema de protección de datos, para corroborar viabilidad.

Elaboración de cuestionarios y materiales

Al elaborar cuestionarios, guías de tópicos y cualquier otro material donde se recaben datos personales, tener en cuenta que:

Además de ser una obligación, el **Aviso de Privacidad** (AP) es el medio por el cual los responsables informan a los titulares qué, cómo y para qué se usarán sus datos personales.

Para mayor información y herramientas sobre la elaboración del AP, visita el sitio web del INAI o asesor legal.

- Contar con AP adecuados que incluyan finalidades para el tratamiento de recabar, supervisar, (recontactar), procesar (capturar, codificar), transferir, etc.
  - En caso de existir, el AP debe incluir la observación por parte del cliente. Y de igual manera, cuando se le transfieren audios, videos, transcripciones, filtros.
  - Los estudios online deben de contar con AP integral y opciones de consentimiento.
  - Los estudios cualitativos siempre deben ir con AP integral o AP con datos sensibles.

Elaboración de cuestionarios y materiales

- Relacionar datos personales en AP con la información recolectada, para facilitar el ejercicio de los derechos ARCO.
- El AP debe ser puesto a disposición del Titular antes de recabar su información.

En la medida de los posible, **disociar** los datos personales.

Recolección de datos

Previo a la recolección de datos, incluir en:

- La capacitación del proyecto, el tema de Protección de datos, así como el de manejo del Aviso de Privacidad.
  - Especificaciones sobre su uso, por ejemplo: debe ser puesto a disposición del Titular antes de recabar su información; debe estar firmado; sólo debe mostrarse; cuando se trate de menores de edad debe ser firmado de consentimiento por padre o tutor, etc.
  - Cómo proceder frente a una queja o una solicitud de Derechos ARCO.
  - Para el seguimiento de los proyectos, determinar qué datos personales se requieren (cuidado con generar controles, controles, y más controles con datos personales).
  - Determinar medidas de seguridad en caso de robo o pérdida de datos personales.

Derechos ARCO: derechos de Acceso, Rectificación, Cancelación y Oposición.

Procesamiento (captura, codificación y procesamiento)

Al procesar la información:

- De no requerirse, disociar datos personales, por ejemplo: no realizar la captura de los datos personales, para evitar bases de datos innecesarios.

- Establecer medidas de seguridad para las bases de datos, por ejemplo: encriptación, separación de datos personales, restringir el acceso a personal no autorizado, etc.

Disociación: se aíslan los datos de manera que por sí mismos no aporten información valiosa de un titular o éste no pueda ser identificable. De esta manera el valor de la base de datos para una persona no autorizada se ve disminuido.

Separación: se separan los activos de información grandes en otros más pequeños, por ejemplo, una base de datos de clientes en dos bases de datos: clientes corporativos y personas físicas.

Entrega de resultados

Al concretar un proyecto con datos personales, corroborar que:

- La transferencia de datos se acompañe del Aviso de Privacidad (AP) con el que se recabaron los datos personales, así como con sus cláusulas de transferencia.

- La entrega de la base de datos personales se haga por medios seguros (archivo cifrado, SharePoint, etc.).

- El envío se realice a la (s) persona (s) designada, es decir, se debe limitar el acceso, para facilitar la protección y el borrado seguro de los datos personales.

Artículo 67 del Reglamento de la LFPDPPP:

"La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado."

Consideraciones generales

El Reglamento de la Ley en su artículo 61 establece las siguientes acciones para la seguridad de los datos personales:

1) Elaborar un inventario de datos y de sus medios de almacenamiento.
2) Determinar las funciones y obligaciones de las personas que traten datos personales.
3) Realizar un análisis de riesgos de los datos personales.
4) Revisar las medidas de seguridad existentes.
5) Realizar un análisis de brecha entre las medidas de seguridad existentes y las necesarias.
6) Elaborar un plan de trabajo para implementar las medidas de seguridad requeridas.
7) Realizar revisiones y auditorías del tratamiento de los datos y de las medidas de seguridad.
8) Mantener capacitado al personal relacionado con el tratamiento de los datos.

Otras consideraciones generales

- Una vez cumplidos los plazos de conservación, proceder con el bloqueo y borrado seguro.

Plazo de conservación
= *Tiempo requerido para llevar a cabo las finalidades del tratamiento*
+ *plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables*
+ *periodo de bloqueo.*

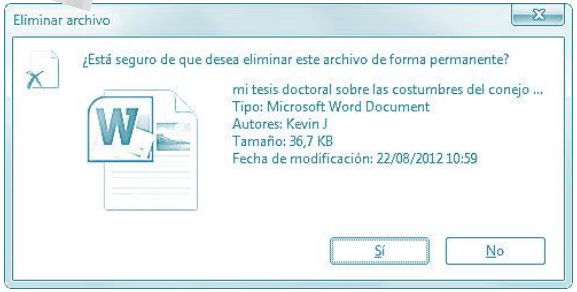
Métodos para el Borrado Seguro de los Datos Personales			
Métodos Físicos		Métodos Lógicos	
Se basan en la destrucción de los medios de almacenamiento		Se basan en la limpieza de los datos almacenados	
Destrucción de los medios de almacenamiento físicos	Destrucción de los medios de almacenamiento electrónicos	Desmagnetización	Sobre-escritura

Otras consideraciones generales

- Documentar el borrado de datos personales.

También considerar

- Accesos restringidos (medidas físicas y electrónicas): cerraduras en los accesos donde existan datos personales, bloqueo de entrada de USB, restringir entrada de celulares, dispositivos con códigos de acceso, información cifrada en dispositivos, etc.



ANEXOS

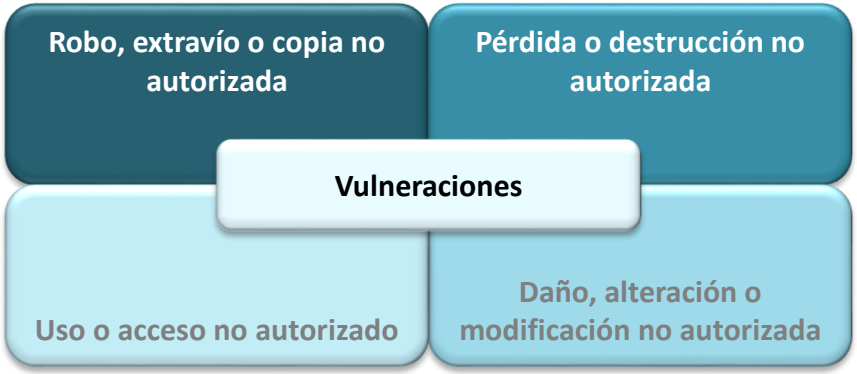
Datos personales recabados

Datos personales recabados		
Datos de identificación y contacto	**Datos biométricos**	**Datos patrimoniales y/o financieros**
Nombre	Imagen del iris	Bienes muebles
Estado Civil Registro Federal de Contribuyentes (RFC)	Huella dactilar	Bienes inmuebles
Clave Única de Registro de Población (CURP)	Palma de la mano	Información fiscal
Lugar de nacimiento	**Datos laborales**	Historial crediticio/Buró de crédito
Fecha de nacimiento	Puesto o cargo que desempeña	Ingresos
Nacionalidad	Domicilio de trabajo	Egresos
Domicilio	Correo electrónico institucional	Cuentas bancarias
Teléfono particular	Teléfono institucional	Números de tarjetas de crédito
Teléfono celular	Referencias laborales Información generada durante los procedimientos de reclutamiento, selección y contratación	Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin)
Correo electrónico	Experiencia/Capacitación laboral	Seguros
Nombre de usuario en redes sociales	**Datos académicos**	Afores
Firma autógrafa	Trayectoria educativa	**Datos migratorios**
Firma electrónica	Títulos	Entrada al país
Edad	Cédula profesional	Salida del país
Fotografía	Certificados	Tiempo de permanencia en el país
Referencias personales	Reconocimientos	Calidad migratoria
Datos sobre características físicas	**Datos sobre pasatiempos, entretenimiento y diversión**	Derechos de residencia
Color de piel	Pasatiempos	Aseguramiento
Color de iris	Aficiones	Repatriación
Color de cabello	Deportes que practica	**Datos legales**
Señas particulares	Juegos de su interés	Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)
Estatura		
Peso		
Cicatrices		
Tipo de sangre		

Datos personales sensibles		
Datos sobre la ideología	**Datos de salud**	**Datos sobre vida sexual**
Posturas religiosas/ ideológicas/morales/ filosóficas	Estado de salud físico presente, pasado o futuro	Preferencias sexuales
Pertenencia a un partido/Posturas políticas	Estado de salud mental presente, pasado o futuro	Prácticas o hábitos sexuales
Pertenencia a un sindicato	Información genética	**Datos de origen étnico o racial**
		Pertenencia a un pueblo, etnia o región

Vulneraciones

- El Reglamento de la LFPDPPP, Artículo 63 establece que existen 4 tipos de vulneraciones de seguridad a los datos personales, que pueden ocurrir en cualquier momento del tratamiento de información personal:



- Es importante identificar los riesgos a los que están expuestos los datos personales, por ejemplo: robo, sustracción, hackers, fuga de información, acceso a información no autorizada, recuperación de datos en equipo obsoleto, borrado de un archivo por error, un incendio.

Borrado seguro por métodos físicos para medios físicos

Nivel de riesgo por sistema de tratamiento	Nivel del estándar	Tamaño máximo del fragmento	Tipo de documento
No recomendable	1. General	Tiras de 12 mm de ancho.	Documentos generales que deben hacerse ilegibles.
No recomendable	2. Interno	Tiras de 6 mm de ancho.	Documentos internos que deben hacerse ilegibles.
Estándar	3. Confidencial	Tiras de 2 mm de ancho. Partículas de 4x80 mm.	Documentos confidenciales.
Sensible	4. Secreto	Partículas de 2x15 mm.	Documentos de importancia vital para la organización que deben mantenerse en secreto.
Especial	5. Alto Secreto	Partículas de 0.8x12 mm.	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas.

Recomendaciones

- ***Guía para el borrado seguro de Datos Personales*** *(Guía de Borrado Seguro)*

- Las Recomendaciones en Materia de Seguridad de Datos Personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013 http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf.

- La Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf.

- El Manual en materia de Seguridad de Datos Personales para MIPYMES y organizaciones pequeñas http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf.

- La Tabla de Equivalencia Funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de Seguridad de Datos Personales http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf.

AMAI 25 AÑOS
INTELIGENCIA APLICADA A DECISIONES

¡Gracias!