AMERICAN CHAMBER/MEXICO

MANUAL DE PROTECCIÓN DE DATOS PERSONALES

A través de este manual, AmCham busca compartir una serie de recomendaciones y propuestas, tanto para usuarios como para empresas, sobre la protección de datos personales, para un uso y manejo seguro de los mismos.

Cuando hablamos de datos personales nos referimos a la información que se relaciona con nuestra persona, nos identifica o nos hace identificables, tal como nuestro nombre, domicilio, correo electrónico, entre otros.[1] El crecimiento exponencial del uso de medios y servicios electrónicos que disponen de nuestra información ha permitido que otros tengan un acceso más fácil a ella, de forma que la obtención de estos datos se ha convertido en una mina de oro en el mercado.

En ese sentido, quienes manejan datos personales tienen una gran responsabilidad: tratar esta información de forma lícita, leal y transparente, y garantizar su seguridad.

De acuerdo con International Telecommunication Union, en 2019,

51%

de la población mundial eran usuarios de internet.[2]

Vivir en un mundo conectado tiene múltiples beneficios para las personas, organizaciones y gobiernos. Estar conectados se ha vuelto necesario para vivir en sociedad, particularmente en el mundo post pandemia.

Conforme al Índice de Transformación Digital 2020 de Dell Technologies, en México el **52% de las empresas** están invirtiendo e innovando y **80% de ellas** realizó un avance rápido en algunos programas de transformación digital.[4]

[1] Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, "¿Qué son los datos personales?", 2021.
[2] International Telecommunication Union, "Measuring digital development: Facts and figures 2020", 2020.
[4] Dell Technologies, "Medimos el progreso de la transformación digital en el mundo", 2020.

Se calcula que durante 2018, cada persona generaba

1.7MB de datos por segundo.[3]

Cada "click", cada "like", cada compra, cada sitio web visitado, genera información que se nos asocia y nos identifica / nos hace identificables (definición legal de datos personales), conformando nuestra huella digital.

Además, muchas veces, sin pensarlo o sin darnos cuenta, concedemos permisos para que distintas aplicaciones y sitios web usen nuestra información.

Todos estos datos e interacciones constituyen nuestra identidad digital y la estamos proporcionando para un uso que desconocemos.

Los datos son un recurso extraordinariamente valioso, pero en muchas ocasiones se ignora que se trata de un derecho humano vinculado directamente con la libertad y dignidad de las personas.

Este derecho se encuentra regulado en la normatividad aplicable tanto para sector privado (LFPDPPP) como público (LGPDPPSO).

En un entorno de creciente digitalización y aumento del cibercrimen, Check Point asegura que **58% de las empresas** reportan haber experimentado un incremento en ataques y amenazas desde el comienzo de la emergencia.[5]

Por otro lado, **México descendió 35 lugares** en el Índice de Ciberseguridad Global durante los últimos seis años. En 2017, ocupaba la posición 28, mientras que, en 2018, el país cayó a la posición 63.[6]

Proteger la información que compartimos y los canales que utilizamos es crucial.

De acuerdo con una encuesta de la consultora MacKeeper, el costo total de los datos de la población en Estados Unidos asciende a los

$48,032,767.87
dólares.[7]

Mientras que, durante 2018 en México, los costos por ciberataques alcanzaron los

$107 millones
dólares.[8]

[3] Domo, "Data Never Sleeps 7.0", 2019.
[5] Dimensional Research for Check Point, "The 'New Normal' is Here to Stay for Some Time: New Survey Reveals Organizations' Security Priorities for 2021 and Beyond", 2020.
[6] Unión Internacional de Telecomunicaciones, "Global Cybersecurity Index", 2018.
[7] MacKeeper, "Most Desired Data: Whose is the most in demand, and how much is it worth?", 2020.
[8] Organización de Estados Americanos, "Estado de la Ciberseguridad en el sistema financiero mexicano", 2019.

Datos personales: Tres aspectos clave

Datos son poder

Los datos son utilizados para fines comerciales o influir en la toma de decisiones.

Quienes usan datos tienen una gran responsabilidad: tratarlos de forma lícita, leal y transparente y garantizar su seguridad.

No puede existir privacidad sin seguridad.

La protección de datos personales es una obligación legal y responsabilidad ética de quien trata los datos personales

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares es el marco legal que obliga a las empresas a cuidar los datos personales.

El Gobierno no es ajeno a esta responsabilidad, también está obligado a resguardar los datos por medio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

De igual forma, todas las organizaciones, públicas y privadas, que tratan datos personales deben observar los principios de licitud, lealtad, consentimiento, calidad, finalidad, proporcionalidad y responsabilidad, así como los deberes de seguridad y confidencialidad.

Cada una de las leyes citadas cuenta a su vez con distintas regulaciones secundarias.

La ciberseguridad es un tema crítico

La pandemia ha provocado que la ciberseguridad sea un tema prioritario debido a la transformación digital de diversos sectores y el incremento de riesgos cibernéticos, como el fishing.

Para garantizar la protección de datos personales, las organizaciones deben:

1. Planear estratégicamente de conformidad con los principios y deberes previstos en la normatividad, contemplando la creación de un programa interno de cumplimiento en la materia.

2. Transitar de la etapa de contención permanente a la prevención de riesgos y la proyección a largo plazo.

"En el entorno digital actual, no basta con respetar la ley, sino que es preciso tener en cuenta la dimensión ética de su tratamiento. La normatividad no puede avanzar al mismo ritmo que lo hace la tecnología, pero sí podemos y debemos asumir estándares éticos que permitan orientar el tratamiento que se da a los datos. Y el primero debe residir en el imperativo categórico más básico: 'no hagas a los demás lo que no quieres que te hagan'.

Si no se incorpora desde los más básicos niveles de conciencia y educación, no hay normatividad ni medida regulatoria posible que impida o disminuya la difusión incontrolable de información con el potencial de causar daños irreparables".

Isabel Davara, Champion de Privacidad de Datos, American Chamber/Mexico

Guía de cumplimiento para las empresas

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares requiere lo siguiente para las empresas:

1. Identificar el flujo lógico de los datos personales que trata la organización a través de un inventario de datos personales. En esta etapa se identifican también los tratamientos de datos existentes en la organización.

2. A partir de la identificación del flujo lógico de datos y tratamientos, crear los avisos de privacidad que la empresa requiera para legitimar el tratamiento de los datos personales, incluyendo cada uno de los elementos informativos previstos por la normatividad aplicable.

3. Cuando sea legalmente requerido, obtener el consentimiento tácito, expreso y/o expreso y por escrito del titular de los datos personales, quien a su vez podrá ejercer en cualquier momento los derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO) al tratamiento de sus datos personales.

4. Designa una persona y/o Departamento al interior de la organización que sea responsable de atender los Derechos ARCO y fomentar la cultura de la protección de datos personales.

5. Utiliza los datos personales sólo para aquellos fines autorizados por los titulares de acuerdo con las finalidades informadas en el aviso de privacidad.

6. Tratar sólo aquellos datos que resulten adecuados, relevantes y necesarios para cumplir con las finalidades del tratamiento.

7 Establecer procedimientos para (i) minimizar el tratamiento de datos personales, (ii) que los datos tratados se encuentren correctos y actualizados en todo momento, (iii) delimitar los periodos de conservación y bloqueo de datos personales de acuerdo con la normatividad aplicable. Una vez concluido el período de bloqueo, realizar la supresión segura de los datos personales.

8 Identificar y regular las comunicaciones de datos personales con terceros, ya sea que se trate de una remisión (responsable a encargado) y/o una transferencia (entre dos responsables).

9 Identificar los tratamientos de datos de alto riesgo y realizar una evaluación de impacto en la protección de datos personales para determinar cuáles serán los riesgos que dichos tratamientos podrían implicar para los derechos y libertades de las personas.

10 Se deben dejar claras las acciones concretas y medidas especiales que tenga implementadas el responsable para garantizar la protección de datos personales de menores de edad y de personas en estado de interdicción y con capacidades diferentes determinadas por ley.

a. Implementar y revisar las medidas de seguridad administrativas, físicas y técnicas para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

b. Para esto, se pueden considerar las recomendaciones emitidas por el INAI y los distintos estándares de seguridad de la información aplicables en el ámbito internacional como las reglas ISO o cualquier otro que resulte aplicable a la organización.

11 Sensibilizar y proporcionar capacitación al interior de la organización en temas de manejo y cuidado de datos personales.

12 Implementar políticas, procedimientos y cualquier mecanismo que permita acreditar el cumplimiento de las obligaciones previstas en la normatividad. Cumplir con la protección de datos implica una responsabilidad proactiva y demostrable por parte de cada organización que trata datos personales.

Consulta: *Documentos (y guías) para el Sector Privado | ABC del aviso de privacidad del INAI.*

Usuarios: Pasos para proteger tus datos

1 Identifica y respalda tus datos

Tu edad, tu domicilio, tu correo, tu patrimonio, además de tus documentos de identidad, son considerados datos personales. Además de guardar los documentos físicos, es recomendable hacer respaldos digitales, en computadoras o servicios de nube[9].

2 Elimina tus datos

Al adquirir un nuevo teléfono inteligente o una computadora y descartar el dispositivo anterior, es recomendable transferir la información y borrar los datos de esos dispositivos[10].

Deberás consultar el manual y el sitio web del proveedor del fabricante para que tus datos se eliminen permanentemente y no sean usados por terceros.

[9] Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Protege tus datos Personales, 2020
[10] Comisión Federal de Comercio, Cómo proteger su información personal, 2016

3 No compartas tu información con nadie

Los sitios bancarios incluyen preguntas de verificación en caso de que no podamos acceder. Esto motiva a los ladrones de identidad a revisar nuestras redes sociales para encontrar información que hayamos compartido.

No compartas tu nombre completo, dirección, ni tus contraseñas en redes sociales.

4 Revisa las responsabilidades que tienen quienes manejan tus datos

Verifica el aviso de privacidad: aquí observarás quién está a cargo de tus datos y cómo los manejan.

Identifica cómo tratan tus datos: se puede especificar en el aviso de privacidad que se permite la transferencia de tus datos a terceros.

Mantente atento a los cambios: la privacidad no se mantiene inmutable, las empresas y el gobierno hacen cambios constantes debido a diversas razones, por ejemplo: adopción de nuevas tecnologías, cambios en regulaciones locales, entre otros[11].

5 Considera usar tu firma electrónica

Debido a la pandemia, la adopción tecnológica se ha acelerado, uno de estos procesos que han sido utilizados es la firma electrónica. Esta firma garantiza que la información se originó de la parte firmante y que no fue alterada. Cualquier cambio a la firma digital invalida el trámite. De igual forma, puedes contemplar el uso de firma electrónica convencional y una firma electrónica avanzada de acuerdo con el tipo de acto jurídico a celebrar.

Con el fin de reducir el contacto, es una opción viable para firma de contratos y otras operaciones que protegen tus datos. Sin embargo, deberás evaluar cuál proveedor se encargará de proteger con mayor seguridad este dato. Otro beneficio de esta firma es que te apoya para realizar trámites para conseguir o reemplazar otros datos personales.

6 Haz valer tus derechos

Una vez que hayas compartido tus datos, la empresa tiene una responsabilidad con su uso. Recuerda que puedes ejercer tus Derechos ARCO en cualquier momento, de acuerdo con el procedimiento que el responsable haya indicado en su aviso de privacidad[12].

A través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)puedes hacer valerlos, mientras que las dependencias locales de transparencia se pueden apoyarte en trámites del sector público.

Por ejemplo, el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales informó que del 23 de marzo al 17 de diciembre atendió 677 denuncias por el uso indebido de datos personales por parte del sector privado y 68 del sector público.

[11] Norton, How to secure your information in the cloud, 2020
[12] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para Titulares de los Datos Personales, 2020

7 Clave, la fortaleza de tus contraseñas

No incluyas información personal en tus contraseñas como apellidos, fecha de nacimiento, nombres de mascotas etcétera porque es fácil de descifrar.

Utiliza caracteres especiales en tus contraseñas y no utilices la misma contraseña en más de un sitio.

Tampoco el mismo NIP para más de una tarjeta.

Para mayor seguridad considera utilizar aplicaciones de contraseñas dinámicas.

" Privacidad, seguridad y ética son componentes imprescindibles de una misma ecuación. El uso lícito de los datos personales es una responsabilidad compartida para el gobierno, las empresas y los titulares".

Isabel Davara, Champion de Privacidad de Datos, American Chamber/Mexico

Fuentes de información:

MacKeeper, "Most Desired Data: Whose is the most in demand, and how much is it worth?", 2020.
International Telecommunication Union, "Measuring digital development: Facts and figures 2020", 2020.
Comisión Federal de Comercio, Cómo proteger su información personal, 2016.
Norton, How to secure your information in the cloud, 2020.
Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, Protege tus datos Personales, 2020.
Unidad de Transparencia del Poder Judicial de la Ciudad de México, Protección de Datos, 2020.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para Titulares de los Datos Personales, 2020.