Conferencia

La protección de datos personales y la ciberseguridad como ejes transversales hacia la nueva normalidad

Mtra. Mireya Arteaga Dirzo

Directora General de Prevención y Autorregulación

noviembre de 2020

Derecho a la protección de datos personales

Elementos por los que destaca la Reforma del Artículo 16 de la CPEUM

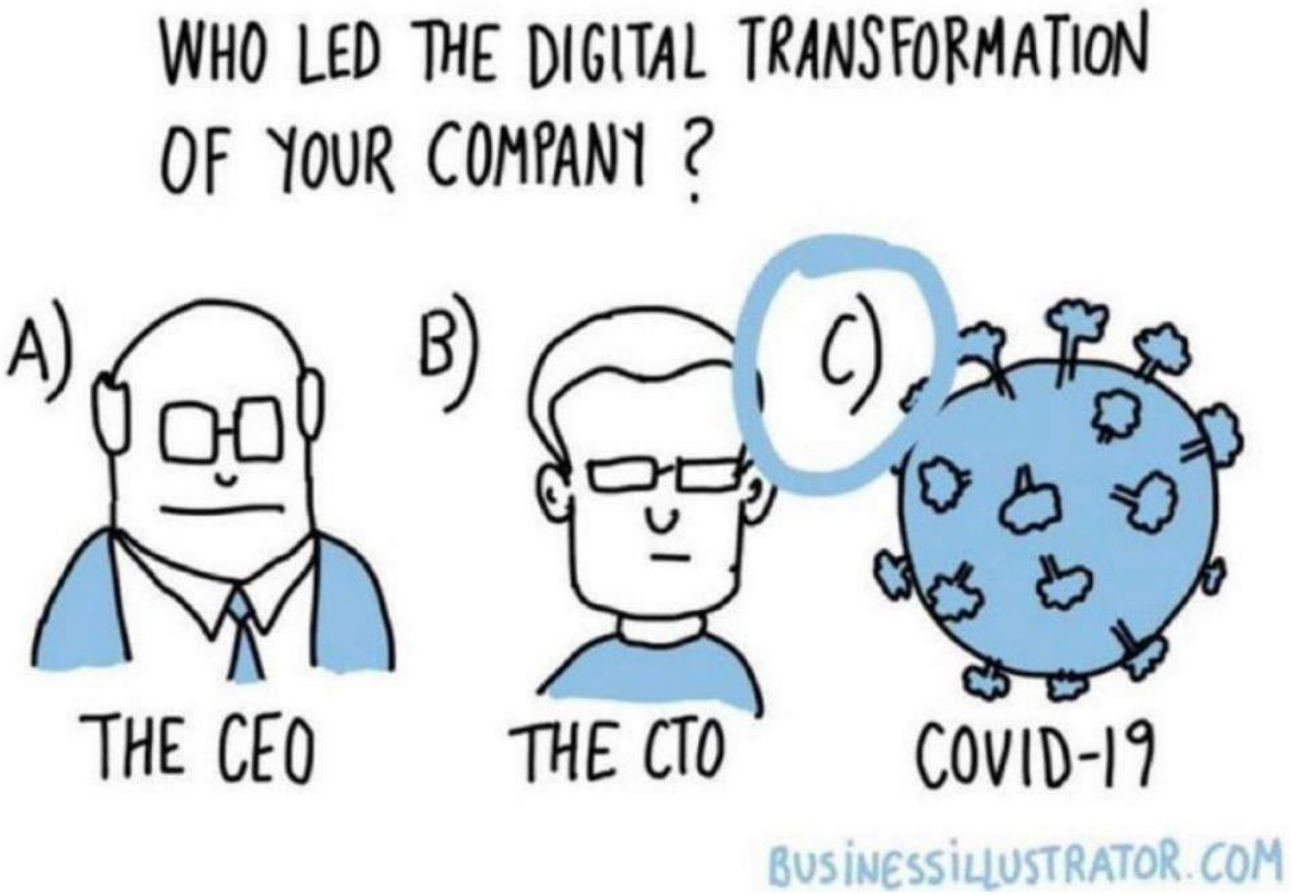
Segundo párrafo Artículo 16

Primera vez que se reconoce de manera explícita en la CPEUM	Derecho de protección de datos personales
Derechos humanos de los individuos	Derechos ARCO
Proceso de construcción institucional	Proveer a las personas de un derecho que garantizará su autonomía para decidir sobre el tratamiento de sus datos
Derecho de PDP implica obligaciones para personas y organizaciones	Cumplir con principios, deberes y obligaciones establecidos en el marco legal
Reconoce que la PDP es un derecho que tiene ciertos límites	

COVID-19 y la transformación

La pandemia de COVID-19 ha **cambiado la forma en que nos conducimos en nuestra cotidianidad,** ya sea en nuestro trabajo o en nuestras actividades sociales.

Esta pandemia ha **impactado en casi todos los aspectos de la economía, la política y, sobre todo, de la sociedad,** siendo el ejercicio de los derechos humanos uno de los temas que más se ha debatido en este contexto



Tratamiento de datos personales ante COVID-19

SALUD

Diagnóstico, contención y tratamiento
Apps COVID-19, robots, IA, blockchain, telemedicina, impresoras 3D, nanotecnología, biología sintética

EDUCACIÓN

Uso de plataformas y herramientas para impartir clases y realizar evaluaciones

INDUSTRIA

Herramientas y mecanismos para el trabajo en casa

COMERCIO

Crecimiento del comercio electrónico (apps, tiendas online)

"NUEVA NORMALIDAD"

Uso de robots, drones, toma de temperatura, reconocimiento facial, certificados de inmunidad

Existe una demanda de **digitalización de procesos y operaciones**, la cual tuvo un avance de **5 años** en los meses que lleva la pandemia.

Las expectativas de crecimiento del mercado global del **Cloud Computing** se estimaban para el 2023 alcanzaría un valor superior a los 174,000 millones de dólares (mdd); según Market Watch, sin embargo, con las necesidades de confinamiento es altamente probable que estas expectativas sean superadas mucho antes.

Principales desafíos en el tratamiento de datos personales ante COVID-19

1. Divulgación de datos personales
2. Cumplimiento de principios y deberes en materia de datos personales
3. Proporcionalidad en la obtención de datos personales
4. Transferencias de datos personales
5. Riesgos en materia de seguridad (vulneraciones)

Medidas de seguridad y tecnologías ante COVID-19

Aplicaciones para el rastreo de contactos

Tecnologías para el reconocimiento facial

Toma de temperatura en espacios públicos y privados

Teletrabajo o trabajo a distancia

Principales riesgos en el tratamiento de datos personales ante COVID-19

Mensajes informativos con enlaces maliciosos

Secuestro de información o *ransomware*

(Programa que bloquea los archivos o dispositivos del usuario y luego reclama un pago en línea anónimo para recuperar el acceso)

Mensajes falsos de solidaridad

Mensajes phishing

(Se comparte con el usuario la dirección electrónica de un sitio web que suplanta la identidad de otro conocido o de interés del usuario para que el atacante robe información o datos personales ingresados por la víctima en el sitio web falso)

Mensajes smishing

(Mensaje SMS que alerta al usuario suplantando la identidad de una institución oficial para compartir un enlace que solicitará datos personales)

Falsos beneficios de supuestos programas sociales

Falsas ofertas de trabajo

Supuestas invitaciones a servicios gratuitos

Ciberdelincuencia: efectos de COVID-19

- **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

Ataques cibernéticos -México

- Los ataques de *phishing* relacionados a COVID-19 aumentaron **350%** desde que inició la cuarentena.

- A nivel mundial, México ocupa la posición número **25** con más ataques de *phishing*.
- En América Latina, ocupa el lugar 12 de acuerdo con Kaspersky.
- México sufrió casi **3 millones de intentos de ataques de virus y malware** durante los primeros tres meses del presente año por medio de amenazas de *phishing.*

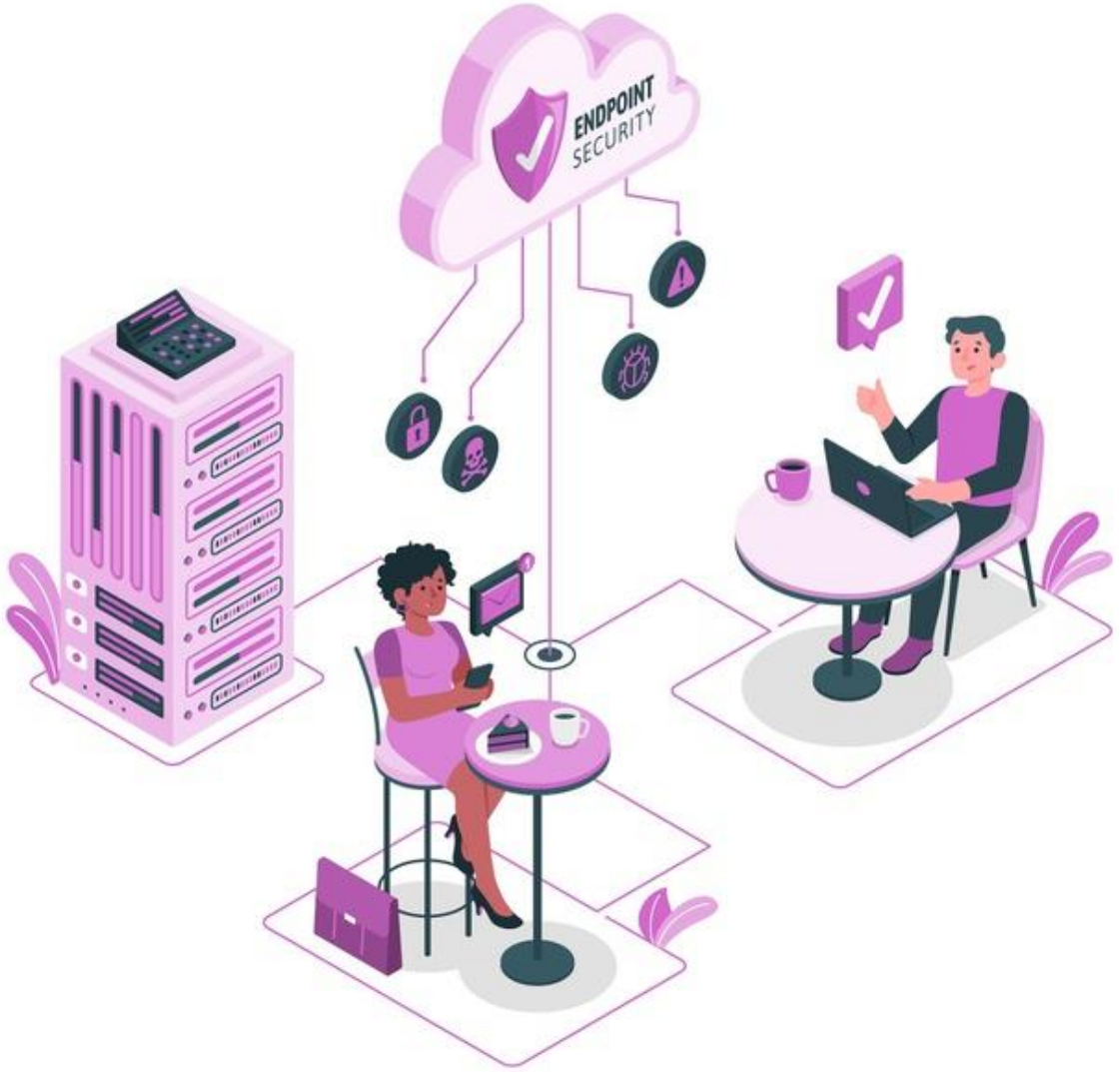
Fuentes: Juan Pablo Castro, director de tecnología y estrategia de ciberseguridad de Trend Micro Latinoamérica, y estudio Fortinet Threat Intelligence Insider Latin America

Recomendaciones phishing

El Instituto ha elaborado un número importante de materiales de difusión sobre el *phishing*, con el objetivo de informar al usuario sobre las distintas modalidades de este fraude cibernético para que pueda reconocer un mensaje de esta clase y se asegure de ciertos elementos antes de proporcionar sus datos personales.

Ciberseguridad

La **ciberseguridad** es el conjunto de *herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías* que pueden utilizarse para proteger los activos de la organización y los usuarios en el **ciberentorno**.



Protección de datos personales y la Ciberseguridad – COVID-19

- Tomando en cuenta que muchas actividades en el entorno digital involucran información personal, es posible afirmar que los **usuarios de Internet pueden valerse del uso de la ciberseguridad para proteger sus datos personales.**

- En ese sentido, se puede advertir que, las tecnologías, en caso de realizar un tratamiento de datos personales, **deberán establecer medidas de ciberseguridad** que permitan proteger los datos contra daños, pérdidas, alteraciones, destrucciones o el uso, acceso o tratamiento no autorizado.

Proyecto de iniciativa de Ley Federal de Ciberseguridad

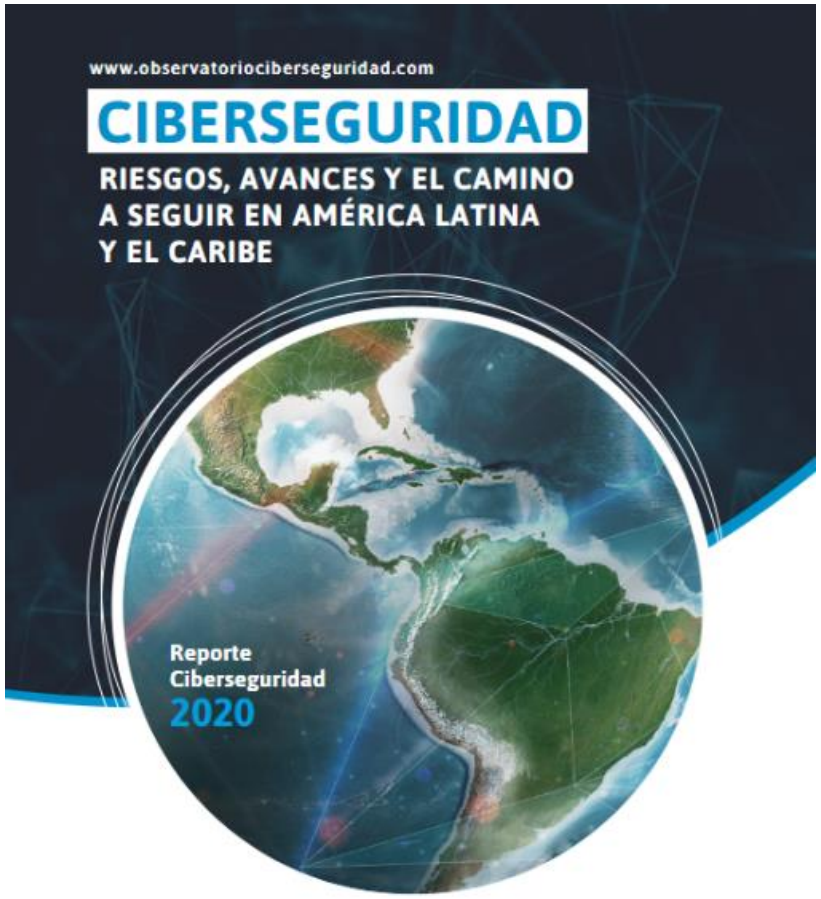
- Establecer **bases de integración para preservar la ciberseguridad**.
- Establece **obligación del Estado para tomar medidas** de monitoreo, prevención y manejo de riesgos, peligros y amenazas interna y externamente del territorio, así como **proteger la infraestructura de información crítica**.
- Presentar **políticas y procedimientos estratégicos**.
- **Sancionar** actividades en el ciberespacio ilegales, criminales.
- **Fomentar la educación de ciberseguridad** en la población de manera concurrente.
- Establecer una **Comisión Permanente de Ciberseguridad** como parte del Consejo Nacional de Seguridad Pública para dar seguimiento y cumplimiento a las disposiciones aplicables por el **Centro Nacional de Ciberseguridad**, el cual, entre otras actividades:
  - Determinará políticas en la materia en coordinación con otras instancias;
  - Expedir lineamientos de ciberseguridad y administración de riesgos, así como los requisitos mínimos que deberán seguir las autoridades de los tres órdenes de gobierno;
  - implementará la protección estratégica sobre la base de un sistema de protección multinivel de ciberseguridad para servicios públicos de diversos sectores

Proyecto de iniciativa de Ley Federal de Ciberseguridad

- Impone **obligaciones a los operadores de red** para garantizar que las redes estén libres de interferencias, daños o acceso no autorizados, adoptando diversas medidas técnicas, tales como:
  - Establecer **sistemas de gestión y normas internas** de funcionamiento para responsables de ciberseguridad;
  - Adoptar **medidas técnicas** para monitorear y registrar estados operativos e incidentes;
  - Adoptar medidas de **clasificación de datos, copias de seguridad y cifrado**.
  - Formular al Centro Nacional de Ciberseguridad **planes de respuesta de emergencia** para incidentes de seguridad y atenderán las vulnerabilidades, malware o ataques cibernéticos;
- El Centro Nacional de Ciberseguridad deberá **informar a las autoridades sobre las ciberamenazas** que enfrenta y establecer **lineamientos de capacitación** para servidores públicos.
- Indica que todas las personas y empresas serán **responsables del uso de sus sitios web**.
- El Centro Nacional de Ciberseguridad deberá establecer requisitos para que empresas proveedoras de ciberseguridad cuenten con **certificados con los más altos estándares**.
- El Centro Nacional contará con una **Estrategia Nacional de Ciberseguridad** que será actualizada al menos cada dos años. Este documento deberá prever el fomento de una cultura de ciberseguridad.
- Se clasifican **4 tipos de delitos con sus respectivas sanciones**.

Ciberseguridad en México
Reporte BID-OEA

- México cuenta con el documento desarrollado en conjunto con la OEA de la **Estrategia Nacional de Ciberseguridad**.
- México cuenta con un **centro para respuesta a incidentes nacional** Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX).
- El gobierno ha promovido varios **eventos en este campo**, como el foro sobre ciberseguridad, con énfasis en el sector financiero, o el curso básico de ciberseguridad para funcionarios públicos ofrecido por la Policía Federal (ahora Guardia Nacional).
- México no cuenta con una **ley dedicada de delito cibernético**, pero el artículo N° 211 del Código Penal prevé el delito informático.
- México ha tenido una **estrategia digital nacional**, parte del Plan Nacional de Desarrollo 2013-2018, cuyo primer objetivo es "aumentar la digitalización de México.
- Actualmente, México ofrece a sus ciudadanos **el portal gob. mx**, que proporciona varios servicios digitales que incluyen identificación, salud y servicios de visado, entre otros.



Para el regreso a la nueva normalidad

Las instituciones y organizaciones deberán aplicar un protocolo de mitigación para proteger a los empleados, clientes y proveedores de la propagación del COVID-19, por lo que se sugiere que se tomen en cuenta **medidas adecuadas para proteger los datos personales sensibles** que podrían recabarse como lo establece:

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

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

Medidas de seguridad ante la nueva normalidad (responsables y encargados)

Algunas **medidas de seguridad** que los responsables y encargados pueden considerar para la protección de los datos personales que se traten como parte de la nueva normalidad:

- Cifrar los datos personales, incluidos los sensibles, es decir, convertir los datos de un formato legible a un formato codificado para que solo se puedan leer o procesar después de haberlos descifrado.
- Realizar un respaldo de la información.
- Utilizar equipos en buen estado.
- Llevar un control de los medios de almacenamiento.
- Utilizar contraseñas robustas en los equipos.
- Guardar las bases de datos en equipos electrónicos con contraseñas seguras.
- Evitar el almacenamiento de los datos en correos electrónicos o unidades compartidas.
- En caso de que los registros sean físicos resguardarlos en archiveros dentro de una oficina con llave.
- El acceso a esta información personal sólo será por el personal autorizado y capacitado para ello.
- Borra la información de forma segura al final de la vida útil de los datos, ya sea triturarla, sobrescribirla o realizar destrucción física, dependiendo el dispositivo seleccionado.

Recomendaciones para los Sujetos Obligados
Nueva normalidad

Para proteger los datos personales de los trabajadores, proveedores y ciudadanía, conoce las recomendaciones para los sujetos obligados para el regreso a la nueva normalidad en materia de protección de datos personales:

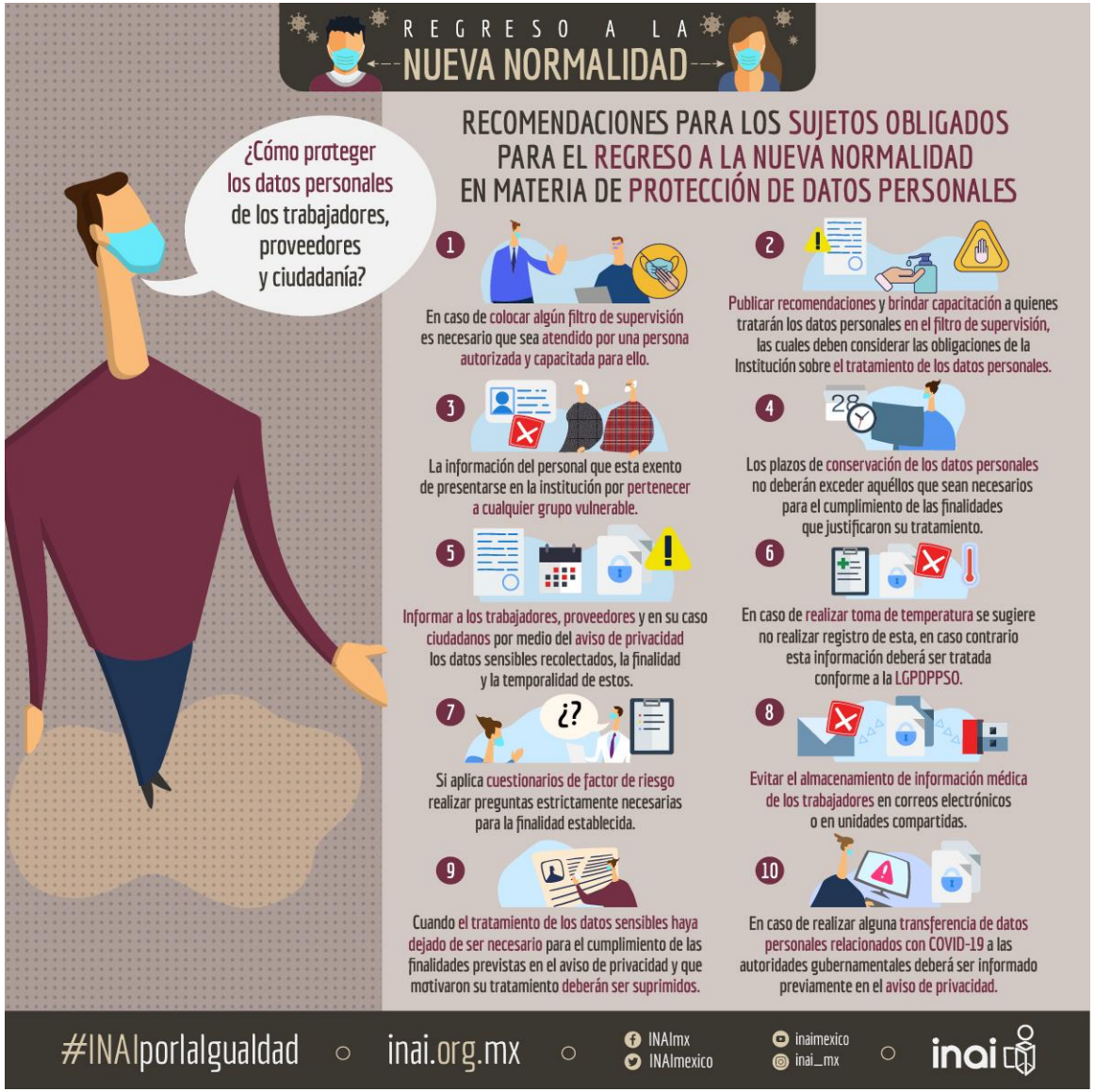
1. En caso de colocar algún filtro de supervisión es necesario que sea atendido por una persona autorizada y capacitada para ello.
2. Publicar recomendaciones y brindar capacitación a quienes tratarán los datos personales en el filtro de supervisión, las cuales deben considerar las obligaciones de la Institución sobre el tratamiento de los datos personales.
3. La información del personal que esta exentó de presentarse en la institución por pertenecer a cualquier grupo vulnerable.
4. Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento
5. Informar a los trabajadores, proveedores y en su caso ciudadanos por medio del aviso de privacidad los datos sensibles recolectados, la finalidad y la temporalidad de estos.

Recomendaciones para los Sujetos Obligados
Nueva normalidad

6. En caso de realizar toma de temperatura se sugiere no realizar registro de esta, en caso contrario esta información deberá ser tratada con forme a la LGPDPPSO.
7. Si aplica cuestionarios de factor de riesgo realizar preguntas estrictamente necesarias para la finalidad establecida
8. Evitar el almacenamiento de información médica de los trabajadores en correos electrónicos o en unidades compartidas.
9. Cuando el tratamiento de los datos sensibles haya dejado de ser necesario para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento deberán ser suprimidos.
10. En caso de realizar alguna transferencia de datos personales relacionados con COVID-19 a las autoridades gubernamentales deberá ser informado previamente en el aviso de privacidad.

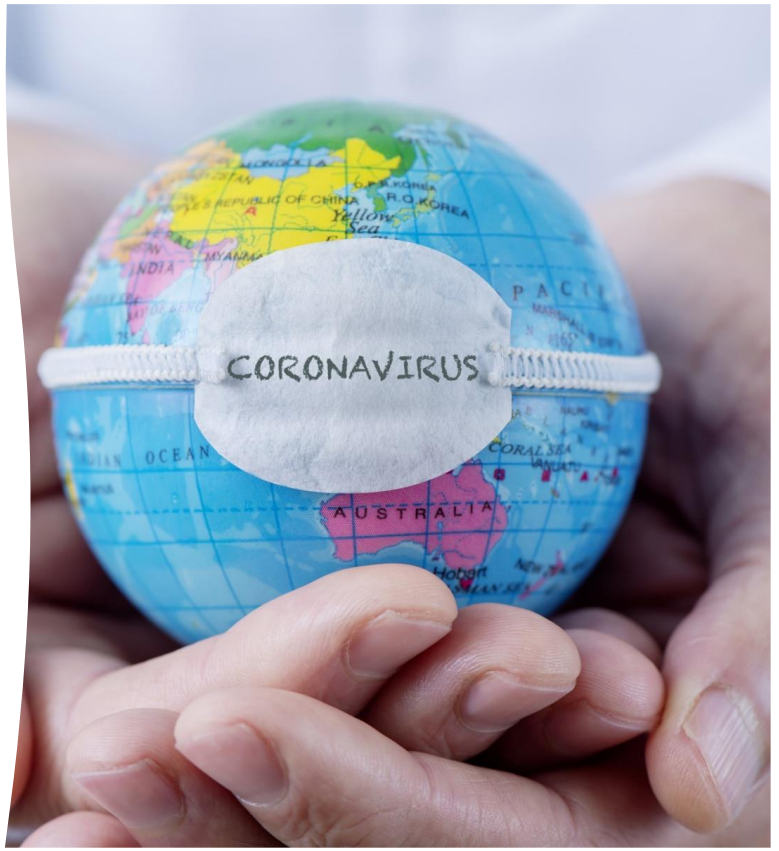
Infografías INAI-Nueva normalidad

Infografías INAI-Nueva normalidad



Retos en la nueva normalidad

- Requerimientos **éticos** relacionados con el desarrollo tecnológico y uso de datos personales.
- Apertura de ventanas de oportunidad para el incremento de la **responsabilidad proactiva de los sujetos obligados** a través de esquemas de cumplimiento legal espontáneo, autorregulación y fomento de mejores prácticas en privacidad.
- Mecanismos legales y fácticos para **armonizar el flujo internacional** de protección de datos personales.
- Fortalecimiento de **mecanismos de cooperación** para facilitar la exigencia del cumplimiento de las disposiciones de datos personales por parte de terceros países y sus jurisdicciones.



Retos en la nueva normalidad

- Desarrollo de **mecanismos de coadyuvancia y/o acompañamiento** de los sectores público y privado y las autoridades de protección de datos personales
- El **uso de tecnologías de seguimiento** de contactos en torno a la vigilancia sanitaria de la epidemia de COVID-19.
- Mayor cuidado en el tratamiento de datos personales dentro de las **aplicaciones móviles.**
- Las **nuevas implicaciones** en el tratamiento de **datos personales sensibles**, que derivado de la pandemia se constituye como un tratamiento principal y necesario en distintos ámbitos.

Retos en la nueva normalidad

- Tratamiento de datos personales a través de **nuevas tecnologías** con énfasis en la geolocalización e identificación de posibles contagios de enfermedades tales como el COVID-19.
- **Reformas normativas necesarias** en materia de protección de datos personales en emergencias sanitarias, por ejemplo, para regular con claridad las medidas intrusivas como el rastreo de contactos o la toma de temperatura para permitir el acceso a establecimientos o el uso de aplicaciones móviles que permiten realizar una autoevaluación del estado de salud individual.
- El **aprovechamiento de datos personales** como insumos para la contención, combate y recuperación de situaciones de emergencia, sobre todo para fines de investigación. Para garantizar la protección de los datos personales en este contexto, es fundamental que estos no se compartan al momento de publicar los resultados de la investigación.

Retos en la nueva normalidad

El artículo *The Acceleration of Digitization as a Result of COVID-19* / Áreas Focales de la digitalización que fueron críticas para la respuesta COVID-19 menciona:

- Un **factor importante es la mejora de la ciberseguridad**, en particular el **manejo de identidades**.
- Adicionalmente otros factores como:
  - Revisión de controles y pruebas,
  - La capacidad de rediseñar procesos.
  - Financiamiento adecuado,
  - El talento adecuado
  - Flexibilidad
- Para prosperar en la nueva normalidad, las organizaciones deben considerar la realización de **evaluaciones de riesgo de los procesos digitalizados y tomar las acciones apropiadas para remediar cualquier brecha de seguridad** identificada. Estas evaluaciones también deben ser un elemento fundamental de las futuras iniciativas de transformación digital, de modo que se puedan implementar los controles adecuados desde el principio"

Acciones INAI

- El **INAI** ha puesto a disposición de la sociedad el "**Micrositio Datos Personales Seguros COVID-19**" sobre la protección de datos personales ante Covid-19.

- Ha publicado **diversos materiales informativos** para titulares, responsables y encargados para el adecuado tratamiento de los datos personales.

- Se han **impartido conferencias** para difundir la importancia de la protección de datos personales ante Covid-19

Acciones internacionales -INAI

El INAI participa de manera proactiva en los distintos foros y redes regionales e internacionales de protección de datos personales compartiendo las acciones emprendidas en el contexto de la pandemia.

El Instituto es miembro del Grupo de trabajo sobre el COVID-19 de la Asamblea Global de Privacidad (GPA) que tiene como objetivo:

- impulsar respuestas prácticas a los problemas de privacidad y protección de datos personales surgidos por la pandemia, y
- difundir información y mejores prácticas.

GPA
Global Privacy Assembly

Aprobación de *"Resolución sobre los desafíos en materia de privacidad y protección de datos que surgen en el contexto de la pandemia de COVID-19"*

Exhorto a autoridades de protección de datos a seguir promoviendo la cooperación en materia de reglamentación, en particular con las autoridades de supervisión pertinentes que no se ocupan de la protección de la privacidad.

Guía para el tratamiento de datos personales en la nueva normalidad laboral

- Facilitar a los sujetos regulados y sujetos obligados el **cumplimiento de la normatividad sobre protección de datos personales**; así como la implementación de acciones que permitan alcanzar dicho cumplimiento ante la emergencia sanitaria de COVID-19.

- Proporcionar información clara, precisa y sencilla para que los **titulares de los datos personales sepan cómo, con qué finalidades y en qué condiciones se pueden tratar sus datos personales**, incluidos los datos de salud en el regreso a la nueva normalidad.

"El acceso a la información veraz y fiable, así como a Internet, es esencial. Deben disponerse las **medidas adecuadas** para que el uso de tecnología de vigilancia para monitorear y rastrear la propagación del coronavirus COVID-19, sea **limitado** y **proporcional** a las necesidades sanitarias y no implique una injerencia desmedida y lesiva para la **privacidad**, la **protección de datos personales**, y a la observancia del principio general de no discriminación"

Derecho a la Salud
Nuevo cuadernillo de Jurisprudencia de la Corte Interamericana N 28


INTERPOL
COVID-19
INTERPOL

GRACIAS

Mtra. Mireya Arteaga Dirzo

Directora General de Prevención y Autorregulación

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

mireya.arteaga@inai.org.mx