La protección de datos personales en tiempos de COVID-19

Dra. Josefina Román Vergara, Comisionada del INAI

PREGUNTAS

1. ¿Cómo se protegería los documentos electrónicos que son los que más estamos usando?

Algunas de las medidas que se pueden implementar para proteger los documentos electrónicos son:

- Respaldos de información[1]: son copias de la información almacenada en un lugar distinto al equipo de cómputo o dispositivo móvil que es de gran utilidad para cuando se pierde información importante o no se tiene acceso al dispositivo.
  La información que se respalda puede respaldarse de dos formas medios físicos o almacenamiento en la nube, ante este último caso se deberán considerar los elementos que en materia de protección de datos personales establece el marco legal.

  Los respaldos deben realizarse de forma frecuentes y manteniéndolas en lugares seguros.

- Uso de contraseñas para controlar el acceso a la información[2]: consiste en los caracteres que permiten el acceso a un sitio, servicio o cuenta del usuario.

  Recomendaciones para las contraseñas
  - Utiliza una contraseña diferente para cada una de las cuentas o dispositivos que utilices.
  - Evita compartir la frase secreta o estrategia para crearlas.
  - No utilices computadoras públicas ya que cualquier persona puede utilizarlas y estas pueden estar infectadas o capturar todas tus pulsaciones de teclado.
  - Utiliza mecanismos de autenticación de dos factores, que consiste en un código de acceso que es enviado al teléfono y que permite el acceso al usuario además de proporcionar su contraseña.

- Establecer permisos o roles de archivos o carpetas, en el caso de compartirlas para que los usuarios puedan editar o solo visualizar la información, de esa forma se establecen políticas de uso.

[1] Disponible en: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_sp.pdf
[2] Disponible en: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_sp.pdf

- Protección de documentos con contraseña, la mayoría de las herramientas permiten establecer contraseñas en los documentos individuales para su acceso.

- Cifrado de documentos[3]: El cifrado ha existido desde hace miles de años, hoy en día es más sofisticado pero el propósito se mantiene, se utiliza para pasar un mensaje secreto de un lugar a otro asegurando que solamente las personas autorizadas podrán acceder y leer el mensaje. Cuando la información no se encuentra cifrada se le llama texto sin formato, esto significa que cualquiera puede leer fácilmente o acceder a dicha información. En la actualidad, el cifrado funciona mediante el uso de operaciones matemáticas complejas y una única clave para convertirla en texto cifrado. La clave es qué bloquea o desbloquea la información, en la mayoría de los casos es a través de una contraseña o código de acceso.

  El cifrado de datos, bloquea el acceso a todo el contenido de un disco y es transparente para el usuario. Los datos se cifran automáticamente cuando se escriben en el disco duro y automáticamente se descifran antes de ser cargados en memoria. Este tipo de medida de seguridad es ideal en unidades USB, unidades flash, etcétera.

- Utilizar transmisiones de documentos con canales de red seguros.
- Uso de herramientas o aplicaciones oficiales.

2. ¿Hasta qué punto prevalece el derecho de la salud pública sobre la protección de datos personales? Sobre todo, ante la situación de que un servidor público dio positivo en COVID 19 y tuvo actividades públicas.

En términos del artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos[4], toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fijen las leyes correspondientes.

También dispone que la ley establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

[3] Disponible en: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201606_sp.pdf
[4] Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Consultada el 13 de agosto de 2020. Disponible en: https://bit.ly/2E1mQoN

Por lo que hace al sector público, el numeral 6 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[5], establece que el Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Relativo al sector privado, el numeral 4 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, dispone que los principios y derechos previstos en dicha Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Ahora bien, los derechos humanos reconocidos que deben optimarse en el mayor grado posible en los términos de progresividad, universalidad, interdependencia, indivisibilidad y pro persona, ello no implica que sean absolutos, por lo que han de determinarse cuáles son los límites legítimos a su ejercicio[6].

No obstante, si el titular de los datos personales tiene conocimiento de un tratamiento indebido de datos personales, es decir, el probable uso ilícito, la divulgación no permitida o el almacenamiento excesivo y desproporcionado de los datos personales, que lleve a cabo el responsable de su protección, sea cual sea el medio físico o electrónico, o algún responsable del sector privado o sector público a nivel federal realizó un uso indebido de datos personales que se proporcionaron para el diagnóstico, atención y seguimiento del COVID-19, se puede acudir al INAI a presentar tu denuncia, por las presuntas violaciones a las disposiciones normativas que regulan el derecho de protección de datos personales.

En su caso, en tratándose de datos personales en posesión de autoridades locales, se deberá acudir a uno de los 32 organismos garantes de los derechos de acceso a la información y de protección de datos personales.

[5] Artículo 6 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consultada el 13 de agosto de 2020. Disponible en: https://bit.ly/2XYcsFk

[6] Tesis 41358, DERECHOS Humanos contenidos en la Constitución y en los Tratados Internacionales, constituyen el parámetro de Control de Regularidad Constitucional, pero cuando en la Constitución haya una restricción expresa al ejercicio de aquellos; se debe estar a lo que establece el texto Constitucional. Gaceta del Semanario Judicial de la Federación. Libro 5, abril de 2014, Tomo I, página 156. Consultado el 13 de agosto de 2020. Disponible en: https://bit.ly/3gVoeYl

3. ¿Es correcto que una empresa obligue a los trabajadores a realizarse la prueba de COVID-19 para ir a trabajar?

En el Acuerdo por el que se establecen los Lineamientos Técnicos Específicos para la Reapertura de Actividades Económicas que emite la Secretaría de Salud Federal se establecen las medidas obligatorias para el retorno o la continuidad de sus labores, en el cual no contempla la aplicación obligatoria de pruebas COVID; sin embargo las Entidad Federativa está emitiendo sus medidas para el regreso a la nueva normalidad en los centros laborales, como es el caso de Jalisco, Sonora y la Ciudad de México que han generado estrategias para la aplicación de pruebas a los empleados de las empresas.

Estado	Aplicación
Ciudad de México	Más de 100 personas al 3% de la totalidad
Jalisco	Menos de 100 empleados 1 de cada 10. Más de 100 empleados 1 de cada de 10.[7]
Sonora	Más de 250 empleados aplican 5% del toral[8]

En el caso de la CDMX, la Administración de la Ciudad de México publicó en la Gaceta Oficial No. 399 Bis, de fecha 10 de julio de 2020, los Lineamientos para la ejecución del plan gradual hacia la nueva normalidad en la Ciudad de México y se crea el comité de monitoreo y su anexo, en los cuales establece que Las personas físicas o morales titulares de los establecimientos o responsables de las actividades que conforme al color del Semáforo Epidemiológico se encuentren operando con un plantilla presencial de 100 o más personas por cada centro de trabajo, deberán realizar a su costa y de manera quincenal, pruebas de detección del virus SARS-CoV2 en RT-PCR de reacción en cadena de la polimerasa, mismas que deberán ser aplicadas en los laboratorios clínicos o lugares autorizados para realizar pruebas COVID-19 en la Ciudad de México, a **por lo menos el 3% de la totalidad de dicha plantilla, ya sea de forma individual o grupa[9]l.**

[7] Plan de Resiliencia ante la Pandemia del Estado de Jalisco, en el apartado Lineamientos para la auto vigilancia.
[8] Guía para la construcción de la nueva normalidad en Sonora COVID-19.
[9] Cuarto de los Lineamientos para la ejecución del plan gradual hacia la nueva normalidad en la Ciudad de México y se crea el comité de monitoreo y su anexo.

Se entenderá por prueba grupal aquella practicada a un grupo de máximo 15 personas (preferentemente que compartan espacios o tengan mayor contacto entre ellos) y consistirá en la toma de muestra a cada una, las cuales se combinarán y procesaran como una sola prueba de reacción en cadena de la polimerasa de diagnóstico del virus

SARS-CoV-2.

Asimismo, deberán asegurarse de que cada uno de los trabajadores del grupo al que se le practicó la prueba se realicen un autodiagnóstico COVID-19, a través de los medios señalados en el numeral 1 del Lineamiento NOVENO BIS. Si la prueba grupal dio positivo de COVID-19, se ordenará resguardo domiciliario al grupo completo y deberá realizarse una prueba individual a cada integrante.

4. ¿Qué sucede cuando se detecta una persona con COVID, y se le pregunta con quien ha tenido contacto? ¿Es correcto que si sales positivo de COVID te obliguen a dar los nombres de las personas con las que tienen contacto?

Tanto en el Lineamiento general para la mitigación y prevención de COVID-19 en espacios públicos cerrados como en los Lineamientos técnicos de seguridad sanitaria en el entorno laboral que publicó la Secretaría de Salud Federal establece la aplicación de un cuestionario de detección de síntomas, en el cual no se contempla la información referente a las personas de contacto en caso de resultado positivo de COVID; sin embargo en el caso de la CDMX en los los Lineamientos para la ejecución del plan gradual hacia la nueva normalidad en la Ciudad de México y se crea el comité de monitoreo y su anexo, se establece que la Secretaria de Salud, en coordinación con la Agencia Digital de Innovación Publica de la Ciudad de México y demás Órganos de la Administración Pública llevaran a cabo un sistema estricto y permanente de vigilancia epidemiológica, con el apoyo de un sistema centralizado desinformación a cargo de la Agencia, para el seguimiento y rastreo epidemiológico que permita la identificación, seguimiento y rastreo de casos positivos y sospechosos de posibles contagios de COVID-19; de su red de contactos o ubicación de zonas de contagio, mediante información recabada de los empleadores, visitas domiciliarias, tamizajes realizados a través de mensajes de texto SMS, vía telefónica de LOCATEL, 911, reportes de contagio

en sectores económicos abiertos y pruebas, a fin de realizar acciones para controlar, contener y minimizar los riesgos de contagios de COVID-19 entre la población.[10]

La información recabada en el sistema de información centralizada permitirá dar seguimiento a los casos de posible contagio o confirmados de COVID-19, localizar e informar a su red de contactos con los que tuvo cercanía y aplicar las pruebas para minimizar la posibilidad de contagio.

5. ¿Qué recomendaciones puede compartir para las personas que utilizan apps médicas o consultas médicas en línea, (considerando muchas veces que el factor común es la prisa y la urgencia de la consulta)?

- Leer con atención las políticas de privacidad de los servicios, software o aplicaciones que sean utilizados para la realización de consultas médicas en línea.
- Las aplicaciones o páginas de internet deben informarle por medio del Aviso de Privacidad, entre otros, el uso y finalidades que darán a sus datos personales y el sitio donde se puede consultar sus términos.
- Descargar el software o aplicación para consultas médicas sólo de sitios oficiales.
- Verificar siempre que el sitio o aplicación que solicita los datos personales corresponda al sitio de la institución u organización que dice ser.
- Evitar proporcionar los datos personales relativos a nuestra salud a través de aplicaciones o medios no oficiales.
- Revisar los permisos que solicita el software o aplicación y analizar si estos son necesarios para el servicio de consulta médica que se está solicitando.
- Evitar ingresar a sitios web a través de enlaces incluidos en correos electrónicos, mensajes de texto o publicados en redes sociales.
- Tomar en consideración que la tecnología utilizada en relación con esta pandemia debe privilegiar la protección de los datos personales sensibles como lo es el estado de salud.

6. ¿En caso de solicitudes que pidan cantidades de servidores públicos de nuestra institución contagiados de COVID, hay obligación de recabarlos?

[10] Octavo De los Lineamientos para la ejecución del plan gradual hacia la nueva normalidad en la ciudad de México y se crea el comité de monitoreo y su anexo.

En el caso que nos ocupa, no hay obligación de recabar datos de salud de una persona física, para dar respuesta a una solicitud de acceso a la información. En este supuesto, no se debe pasar desapercibido que para identificar la cantidad de servidores públicos contagiados de COVID, es necesario obtener una evidencia documental que respalde el diagnóstico, lo que generaría un nuevo tratamiento de datos sensibles, mismo que no se encuentra previsto en la contratación de ningún servidor público.

Es preciso aclarar que, conforme a la fracción X del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los datos que describan el estado de salud presente o futuro de cualquier servidor público, son considerados datos sensibles[11], por lo que, por regla general no pueden tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la LGPDPPSO[12].

De esta manera, no se identifica una obligación de recabar dicha información, para la atención de una solicitud de acceso. Ahora bien, en caso de que el responsable requerido cuente con facultades para obtener el estado de salud de las personas, se deberán de implementar medidas de seguridad que resguarden dicha información y, solo podrán proporcionarse siempre que hayan sido sujetos a procedimientos de disociación, o únicamente refieran a datos estadísticos respecto a la cantidad de contagiados a partir del análisis de la información recolectada de manera lícita, proporcional y consentida por el titular.

7. Grabar una conferencia virtual o una junta o reunión de trabajo donde se ven rostros, es un dato sensible, ¿se necesita consentimiento de forma expresa? ¿Y si es así como se recomienda recopilarla?

Dentro de los datos personales, existen además lo datos personales sensibles: Aquellos datos que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos

[11] Art. 3, fracción X de la LFPDPPSO. Datos personales sensibles: 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. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

[12] Artículo 7 de la LGPDPPSO

que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, etc. Sin embargo, el ROSTRO de una persona durante una conferencia virtual NO se puede considerar en sí mismo como datos sensibles, solamente como DATO PERSONAL, por lo que para poder grabar una junta virtual NO es necesario contar con CONSENTIMIENTO EXPRESO, sino informar al titular mediante un AVISO DE PRIVACIDAD, que se va a recabar su dato personal.

Un aviso de privacidad es un documento físico, electrónico o en cualquier otro formato (por ejemplo, sonoro), a través del cual el responsable informa al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales. A través del aviso de privacidad se cumple el principio de información que establece la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo la Ley) y su Reglamento.[13]

El aviso de privacidad tiene como propósito principal establecer y delimitar el alcance, términos y condiciones del tratamiento de los datos personales, a fin de que el titular pueda tomar decisiones informadas con relación a sus datos personales y mantenga el control y disposición de la información que le corresponde.

Asimismo, el aviso de privacidad permite al responsable transparentar el tratamiento o uso que da a los datos personales que están en su posesión, así como los mecanismos que tiene habilitados para que los titulares ejerzan sus derechos con relación a su información personal, lo que, sin duda, fortalece el nivel de confianza del titular con relación a la protección de sus datos personales. En este caso ANTES de realizar la grabación, se debe poner a disposición del titular el AVISO DE PRIVACIDAD.

8. ¿Podría ahondar en los términos de geolocalización y georreferenciación?

La **geolocalización** es el proceso de encontrar, determinar y proporcionar la ubicación exacta de una computadora, dispositivo de red o equipo. Permite la ubicación del dispositivo según las coordenadas geográficas y las medidas. La geolocalización suele utilizar el sistema de posicionamiento global (GPS) y otras tecnologías relacionadas para evaluar y especificar ubicaciones geográficas.

[13] Artículos 15 y 16 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

La geolocalización proporciona la ubicación de un dispositivo, pero generalmente se usa en una variedad de aplicaciones para ayudar a ubicar a los usuarios humanos. La geolocalización funciona a través de un GPS[14] preconstruido en un dispositivo que propaga las coordenadas longitudinales y latitudinales del dispositivo. Las coordenadas se identifican en un mapa para proporcionar una dirección completa que generalmente incluye un país, ciudad, pueblo / colonia, nombre del edificio y dirección.

Por otro lado, la **georreferenciación** es el uso de coordenadas de mapa para asignar una ubicación espacial a entidades cartográficas. Todos los elementos de una capa de mapa tienen una ubicación geográfica y una extensión específicas que permiten situarlos en la superficie de la Tierra o cerca de ella. La capacidad de localizar de manera precisa las entidades geográficas es fundamental tanto en la representación cartográfica como en SIG[15].

Aunque a priori puedan parecer lo mismo, existen varias diferencias entre los mismos, tanto en su definición como en sus aplicaciones. La Universidad Politécnica de Valencia define la georreferenciación, como un proceso por el cual se dota de un sistema de referencia de coordenadas terreno a una imagen digital que originariamente se encuentra en coordenadas pixel.

Por su parte, la geolocalización, se define como la identificación de la ubicación de un dispositivo por ejemplo un radar, teléfono móvil o cualquier aparato tecnológico conectado a internet. Está relacionada con los sistemas de detección de posición, pero añade datos como información de la zona, calles, locales, etcétera.

9. Es válido "exentar" el consentimiento expreso de los titulares con la finalidad de implementar un cuestionario donde se solicite información sobre el estado de salud general durante esta pandemia, es decir, ¿es necesario que los titulares de los datos otorguen de manera expresa su consentimiento?, o bien, ¿Se pueden invocar las causales de excepción referidas por la normatividad?

[14] Sistema de Posicionamiento Global. https://www.gps.gov/systems/gps/spanish.php
[15] Sistema de Información Geográfica. https://www.ceibal.edu.uy/storage/app/media/Marco-teorico-Cartografia-SIG.pdf

El 27 de marzo de 2020, en el Diario Oficial de la Federación (DOF), el Titular del Poder Ejecutivo Federal declaró diversas acciones extraordinarias en materia de salubridad general para combatir la enfermedad grave de atención prioritaria generada por el virus SARS-CoV2 (COVID-19).

El 30 de marzo el Consejo de Salubridad General emite la "Declaratoria de Emergencia Sanitaria por Causa de Fuerza Mayor" con vigencia del 30 de marzo al 30 de abril.

Con base en estos antecedentes, se puede considerar que derivado del virus SARS-CoV2 (COVID-19), el gobierno federal declaró situación de emergencia, por lo cual se configura la excepción contenida en la fracción V del artículo 10 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares[16] (Ley Federal), mediante la cual, si existe una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes, NO SERÁ NECESARIO EL CONSENTIMIENTO para el tratamiento de sus datos personales, esto sin dejar de observar lo estipulado en el artículo 17 segundo párrafo del Reglamento de la ley Federal de Protección de Datos Personales en Posesión de Particulares [17] el cual a la letra dice:

[… Artículo 17. En términos de lo dispuesto por los artículos 10, fracción IV y 37, fracción VII de la Ley, no se requerirá el consentimiento tácito o expreso para el tratamiento de los datos personales cuando éstos deriven de una relación jurídica entre el titular y el responsable.

No resulta aplicable lo establecido en el párrafo anterior cuando el tratamiento de datos personales sea para finalidades distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular…]

Por otra parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[18] (Ley General), enuncia en su artículo 22 fracción VI, que cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes, el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.

De lo anterior, se puede observar que ambas legislaciones en materia de Protección de Datos Personales del sector público y privado contemplan causales de excepción para recabar el

[16] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
[17] http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf
[18] http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

consentimiento de los titulares para el tratamiento de sus datos personales cuando EXISTA UNA SITUCIACIÓN DE EMERGENCIA, como es la SITUACIÓN ACTUAL.

Ahora bien, es importante hacer notar que, para el caso de los datos recabados en este supuesto, cuando sea necesaria realizar una transferencia sin el consentimiento de los titulares, la Ley Federal en su artículo 37 fracción II y V; y en la Ley General en su artículo 70 fracción VIII, contemplan causales de excepción para las transferencias sin consentimiento de los titulares.

10. ¿En el caso de la bitácora de registro de temperaturas hay algún tiempo recomendado para su destrucción? ¿O se toma el mismo tiempo de resguardo que la documentación de su naturaleza?

Comprobar si el estado de salud de los trabajadores puede constituir un peligro para ellas mismas, para el resto del personal, o para otras personas relacionadas con la organización en la que se labora, constituye una medida relacionada con la vigilancia de la salud de los trabajadores que, conforme a la legislación laboral, resulta obligatoria para el empleador. En todo caso, el tratamiento de los datos obtenidos a partir de las tomas de temperatura debe respetar la legislación de protección de datos y, por ello y entre otras obligaciones, debe obedecer al principio de finalidad, es decir que deberá ser recabada únicamente para la finalidad específica de contener la propagación del coronavirus, limitarse a esa finalidad y no extenderse a otras distintas, y no podrá ser mantenida dicha información más del tiempo necesario para la finalidad para la que se recaban.

Ahora bien, por lo que hace al establecimiento de plazos y criterios de conservación de los datos en los casos en que sean registrados, para el caso de las bitácoras de toma de temperatura, dadas las finalidades del tratamiento, este registro y conservación no debieran producirse, salvo que pueda justificarse suficientemente ante la necesidad de hacer frente a eventuales acciones legales derivadas de la decisión de denegación de accesos a ciertos lugares.