



# RECOMENDACIONES

Para los tratamientos de datos personales relacionados con la emergencia sanitaria por COVID-19



El 29 de julio de 2020, el Presidente de la Suprema Corte de Justicia de la Nación emitió el Acuerdo General de Administración II/2020 (AGA II/2020), con el propósito de establecer los lineamientos de seguridad sanitaria durante la emergencia generada por el virus SARS-CoV2 (COVID-19).

El AGA II/2020 estableció, entre otras cosas, que los datos personales que se recaben por las áreas conforme a esa normativa y la Guía Operativa, serán estrictamente protegidos y tratados en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO).

Por su parte, la Guía Operativa desarrolló diversas actividades complementarias para prevenir la transmisión del COVID-19 en el proceso del retorno paulatino a las actividades presenciales.

Ambos documentos reconocen una serie de medidas que deberán observar las áreas para la programación de actividades presenciales, así como obligaciones relacionadas con la comunicación de diagnósticos confirmados positivos de COVID-19 o síntomas asociados a dicha enfermedad. Por sus propias características, la materialización de estos deberes se considera un tratamiento de datos personales sensibles, en términos de la LGPDPSO.

Por lo anterior, las áreas que se involucren en el tratamiento de datos personales relacionados con la emergencia sanitaria por COVID-19, deben atender las siguientes recomendaciones.

# PRIMERA

## REPORTAR LOS TRATAMIENTOS DE DATOS PERSONALES PARA EL INVENTARIO INSTITUCIONAL



En la **GUÍA DE PROTECCIÓN DE DATOS PERSONALES**, distribuida por la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTSIJ) en febrero de 2019, se desarrollaron diversos conceptos relevantes en la materia.

Entre otras cosas, se precisó que el tratamiento de datos personales debe considerarse como cualquier operación manual o automatizada aplicada a los datos personales. Sirven como ejemplo, de manera enunciativa, los siguientes supuestos: obtención, uso, registro, organización, conservación, difusión, transferencia, etcétera.

Además, se definieron como datos personales sensibles aquellos que afecten la esfera más íntima de su titular y cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Entre otros, se consideran sensibles

aquéllos que puedan revelar aspectos como el estado de salud pasado, presente y futuro.

En ese sentido, se recomienda que las áreas que recaben datos personales relacionados con el AGA II/2020, particularmente sobre diagnósticos confirmados positivos de COVID-19 o síntomas asociados a dicha enfermedad, soliciten a la UGTSIJ su registro en el **INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES** y desplieguen las gestiones respectivas.

# SEGUNDA

## TRATAR LOS DATOS PERSONALES SENSIBLES CONFORME A LOS PRINCIPIOS LEGALES



La protección de datos personales es un derecho fundamental que permite a las personas conocer y controlar su información cuando la otorgan a las instituciones públicas y/o privadas, así como asegurarse de que se utilice de forma adecuada.

Por ello, los tratamientos deben sujetarse a ciertos principios y medidas de seguridad para salvaguardar el derecho que tienen los titulares a la protección de sus datos personales y a la libre determinación de su información.

En la **GUÍA BÁSICA PARA LAS PERSONAS QUE INTERVIENEN EN EL TRATAMIENTO DE DATOS PERSONALES**, divulgada por la UGTSIJ en febrero de 2020, se puntualizó que, como poseedores de datos personales, deben tratarlos, cuando menos, bajo los siguientes parámetros:

- **LEALTAD.** Privilegiar la protección de los intereses del titular y su expectativa razonable de privacidad, evitando obtener sus datos personales a través de medios engañosos.

- **PROPORCIONALIDAD.** Tratar únicamente los datos personales que resulten relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
- **RESPONSABILIDAD.** Guardar confidencialidad de los datos personales y mantenerlos en un lugar seguro, fuera del alcance de terceros; además de observar las medidas de seguridad recomendadas para los tratamientos respectivos.

# TERCERA

## PROPORCIONAR EL AVISO DE PRIVACIDAD



En virtud de que la protección de datos personales es un derecho fundamental, el consentimiento de sus titulares es un requisito legal para realizar los tratamientos. Por regla general, se puede obtener el consentimiento cuando, habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

El aviso de privacidad es el documento que se pone disposición de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben datos personales y con el objeto de informar a su titular los propósitos de su tratamiento. Debe ser sencillo, en lenguaje claro y con un diseño que facilite su lectura y comprensión.

Por ello, se recomienda poner a disposición de los titulares el aviso de privacidad simplificado en el momento en que se recaban sus datos personales sobre diagnósticos confirmados positivos de COVID-19 o síntomas asociados a dicha enfermedad, así como informales que pueden consultar el aviso de privacidad integral en el portal de institucional, a través del siguiente enlace: [https://www.scjn.gob.mx/sites/default/files/pagina\\_transparencia/documento/2020-08/API-SCJN-COVID-19.pdf](https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2020-08/API-SCJN-COVID-19.pdf)



# CUARTA

## COMPARTIR LOS DATOS PERSONALES DE FORMA SEGURA



Una de las medidas contempladas por el AGA II/2020 y la Guía Operativa es la de comunicar información relacionada con el estado de salud de las personas, en cuyo caso se prevé la intervención de superiores jerárquicos, titulares de áreas y la Dirección General de Servicios Médicos.

Ante esta circunstancia, se recomienda observar las directrices desarrolladas en la **GUÍA PARA LA TRANSMISIÓN SEGURA DE DATOS PERSONALES**, que la UGTSIJ divulgó el pasado mayo de 2020, cuya finalidad es ofrecer mecanismos para que las áreas realicen transmisiones adecuadas de datos, implementando medidas de seguridad de carácter administrativo y/o tecnológico, en términos de las disposiciones de la LGPDPPSO.

Se trata de medidas básicas que garantizan, cuando menos, que la información no quede expuesta a personas ajenas al emisor y al destinatario.

# QUINTA

## REPORTAR Y REGISTRAR CUALQUIER VULNERACIÓN



Las vulneraciones a la seguridad de los datos personales pueden ocurrir en cualquier etapa del tratamiento (registro, uso, aprovechamiento, conservación, etcétera). En ese sentido, por vulneraciones se deben entender, por lo menos, las siguientes circunstancias respecto de datos personales (en particular), bases de datos y/o sistemas que los albergan (en general):

1. La pérdida o destrucción no autorizada;
2. El robo, extravío o copia no autorizada;
3. El uso, acceso o tratamiento no autorizado; o
4. El daño, la alteración o modificación no autorizada.

Para garantizar la atención adecuada de cualquier vulneración de datos personales, se recomienda que cada área cuente con su propia Bitácora de Vulneraciones y observe el **INSTRUCTIVO PARA REGISTRAR Y REPORTAR VULNERACIONES DE DATOS PERSONALES** que la UGTSIJ divulgó en agosto de 2020.

Es importante reiterar que los datos personales de salud relacionados con la atención de la emergencia sanitaria se consideran sensibles, por lo que se deberá informar sobre cualquier tipo de vulneración, incluso, a sus titulares, conforme se señala en el instructivo referido.

**Dudas o comentarios dirigirse a:**

**Unidad General de Transparencia y Sistematización  
de la Información Judicial**

Correo electrónico:  
[datospersonales@mail.scjn.gob.mx](mailto:datospersonales@mail.scjn.gob.mx)



**Suprema Corte**  
de Justicia de la Nación