Suprema Corte
de Justicia de la Nación

Guía para la
TRANSMISIÓN SEGURA
de datos personales

Unidad General
de Transparencia
y Sistematización de
la Información Judicial

OCTUBRE 2025

I. Propósito

La finalidad de esta Guía es ofrecer recomendaciones para que los órganos y áreas de la Suprema Corte de Justicia de la Nación (SCJN) realicen transmisiones seguras de datos personales cuyo tratamiento está bajo su responsabilidad, implementando medidas de seguridad básicas de carácter administrativo, físico y técnico, en términos de las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Estas medidas tienen como referencia el principio de *proporcionalidad,* que mandata que los responsables deben tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento (artículo 19 LGPDPPSO). Evitando, en la medida de lo posible, recabar datos no relevantes para el tratamiento o realizar tratamientos que no se justifiquen con las atribuciones y/o funciones conferidas por la normativa institucional.

También, estas medidas garantizan el principio de *lealtad*, que ordena privilegiar en todo momento la protección del interés del titular por el que otorgó sus datos y su expectativa razonable de privacidad (artículo 13 LGPDPPSO).

Para los propósitos de esta Guía, debe entenderse por transmisiones toda comunicación de datos personales fuera del área responsable de su tratamiento, ya sea que éstas se hagan a otros órganos o áreas de la SCJN o incluso, a otras instituciones (transferencias).

Conforme a los principios en la materia, es necesario que los responsables de los tratamientos de datos personales revaloren la necesidad y/o pertinencia de transmitirlos ya que, sin las medidas adecuadas, aumenta el riesgo de divulgación de información confidencial. En caso de ser necesario e indispensable, deberán adoptar las medidas de seguridad recomendadas en esta Guía, así como aquellas que contribuyan a preservar su confidencialidad.

Finalmente, es importante contemplar que el principio de ***responsabilidad*** recae, esencialmente, en los órganos y áreas de la SCJN que recaban, tratan y conservan los datos personales conforme a sus atribuciones y/o funciones específicas. Las medidas de seguridad que aquí se proponen contribuyen a cumplir con dicho principio y a detectar los riesgos potenciales cuando se transmiten los datos personales.

II. TRANSMISIONES EXTERNAS A TRAVÉS DE TRANSFERENCIAS

Las transferencias son toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado (artículo 3, fracción XXX LGPDPPSO). Una transferencia es una transmisión de datos personales a una institución diversa a la SCJN.

Un ejemplo de este tipo de transferencias son las que se realizan al comunicar datos personales a las aseguradoras para la obtención de los beneficios pactados; o la comunicación de bases de datos personales que se realizan a otras instituciones o empresas cuando se comparten eventos o cursos; entre otras.

Además de las medidas de seguridad que se recomiendan en esta Guía y que se desarrollan más adelante, las transferencias deben tener un procedimiento especial de acuerdo con los estándares de la propia LGPDPSO.

Algunas de las cuestiones que se deben observar, son las siguientes:

1. Formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con las atribuciones del área responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. Esta formalización no es necesaria en los siguientes casos:
   - **i)** Que la transferencia sea nacional y se realice entre responsables en virtud de sus atribuciones y/o el cumplimiento de una disposición legal; o
   - **ii)** Que sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional (artículo 60 LGPDPPSO).
2. Que el receptor se comprometa a garantizar la confidencialidad de los datos personales y a utilizarlos únicamente para los fines que fueron transferidos (artículo 61 LGPDPPSO).
3. Que el receptor se comprometa a proteger los datos personales conforme a los principios y deberes que establece la ley en la materia (artículo 62 LGPDPPSO).

Adoptar estas medidas, junto con las acciones para proteger los archivos físicos y electrónicos a través de los que se comparten datos personales, refuerza el principio de *responsabilidad*, en tanto las áreas que transfieren datos personales se aseguran de haber hecho todo lo legalmente exigible para garantizar la confidencialidad de la información.

III. Transmisión de datos personales en archivos físicos

Las acciones diagnósticas realizadas por la Unidad General de Transparencia y Sistematización de la Información Judicial para la elaboración del *Documento de Seguridad*, revelaron que la transmisión de datos personales de manera física entre los órganos y áreas de la SCJN es una actividad cotidiana y, en algunas ocasiones, necesaria para el despliegue de las atribuciones y/o funciones que les confiere la normativa interna.

Estas acciones también mostraron que existen diversas áreas de oportunidad para que las transmisiones físicas se realicen bajo medidas de protección que aseguren la confidencialidad de los datos personales que se comparten.

Ejemplos de transmisiones físicas son listas de asistencia, datos de vehículos, currículums vitae, exámenes de ingreso (como los psicométricos), datos de contacto, entre otros. En estos casos, los datos personales pueden reflejarse en un documento anexo o en el propio texto de los oficios a través de los cuales se comparten. También deben considerarse contenedores físicos como discos duros, medios ópticos (CD, DVD, y BlueRay) y memorias USB, a través de los cuales se transmiten datos personales.

Algunas de las medidas más recomendables para la transmisión de datos personales en forma física implican, al menos, lo siguiente:

1. Realizarlas en **sobre cerrado**, para asegurar que su revisión la realice solamente su destinatario e implementar **controles de seguridad físicos** necesarios (por ejemplo: sellos) que aseguren que el sobre donde se encuentra la información no ha sido quebrantado durante el traslado.
2. Incluir la **advertencia** de que contiene información confidencial que no puede ser reproducida, compartida y/o conservada por ningún medio, y que, una vez que cumpla

su finalidad, ésta deberá ser devuelta de manera íntegra al área remitente en la medida que esto sea posible. Esta propuesta puede quedar reflejada en un etiquetado de la siguiente manera:

CONFIDENCIAL

Esta información deberá ser devuelta al área remitente una vez que cumpla su finalidad y no puede ser reproducida, compartida y/o conservada por ningún medio

3. El personal autorizado **debe custodiar**, en todo momento, el traslado de la información en formatos o contenedores físicos hasta su destino, ninguna otra persona puede suplir esta responsabilidad.

Estas medidas administrativas evitarán que los datos personales queden expuestos en el proceso de la transmisión y, en principio, brindará certeza al destinatario para que no se vulnere su confidencialidad.

IV. TRANSMISIÓN DE DATOS PERSONALES EN ARCHIVOS ELECTRÓNICOS

Algunas transmisiones de datos personales entre los órganos y áreas de la SCJN -e incluso algunas con otras instituciones- se realizan de manera electrónica, a través del envío de archivos adjuntos en correos electrónicos y/o usando sistemas o aplicaciones institucionales.

Por ejemplo, información médica para la realización de actividades sociales y culturales; aquella enviada para utilizar los beneficios de los seguros contratados; la que se comparte a través de correos electrónicos, entre otras.

Existen varias medidas técnicas para proteger datos personales que se comparten a través de archivos electrónicos. Una medida básica y de fácil implementación es la **encriptación de los archivos**.

Encriptar o cifrar los archivos es un procedimiento que impide que la información sea visible y servible para los usuarios no autorizados a conocerla. Para ello, es posible establecer una contraseña de acceso a los archivos.

1. Encriptar archivos Office

Para encriptar los archivos elaborados en programas de Office (Word, Excel, Power Point), es necesario seguir los siguientes pasos:

Paso 1. Abrir el documento. Ir a "Archivo" y luego a "Información".

Paso 2. Dar *clic* en "Proteger documento/libro".

Paso 3. Seleccionar "Cifrar con contraseña".

Paso 4. Escribir la contraseña y luego confirmarla.

Paso 5. El documento ha quedado protegido con contraseña.

2. Encriptar archivos con herramienta 7zip

Para encriptar los archivos en cualquier formato (por ejemplo, en PDF) es necesario llevar a cabo el siguiente procedimiento:

Paso 1. Abrir el explorador de archivos y seleccionar el(los) archivo(s) a encriptar.

Paso 2. Dar clic secundario (botón derecho del ratón en la mayoría de los casos) y seleccionar la opción de 7zip-> Añadir al archivo….

Paso 3. Seleccionar formato de archivo a comprimir (zip, 7z, tar, etc.).

Paso 4. En el apartado de *"encriptación"* escribir la contraseña en los dos campos indicados para ello.

Paso 5. Dar clic en "Aceptar". 7zip empaqueta y crea un archivo con el nombre seleccionado para el mismo, el cual se ha protegido correctamente mediante contraseña.

Con este procedimiento se logran proteger archivos tipo PDF, sin necesidad de tener la licencia de Adobe Acrobat Professional.

Para encriptar archivos a través de esta herramienta, se requiere contar con el programa 7zip, el cual debe solicitarse formalmente a la Dirección General de Tecnologías de la Información (DGTI) mediante el canal de atención de la mesa de servicios, para proceder a su instalación.

3. Recomendaciones para elegir contraseñas de encriptación

Cualquier contraseña o clave de acceso a utilizarse, deberá construirse de forma robusta, conforme a lo siguiente:

- Contar con una longitud de mínimo 12 caracteres.
- Incluir por lo menos: una letra mayúscula, una letra minúscula, un símbolo especial y un número.
- Evitar el uso de palabras comunes o datos personales.

Las claves de acceso son intransferibles, pudiéndose compartir única y exclusivamente a los destinatarios de los archivos electrónicos con la finalidad de que los puedan visualizar.

Se recomienda que la contraseña que se elige para encriptar los archivos electrónicos se comparta en otro correo electrónico para disociar la protección del archivo con la medida de seguridad adoptada o, incluso, a través de otro medio de comunicación entre el emisor y el receptor.

4. Transmitir archivos a través de OneDrive

Otra forma de transmitir de forma segura archivos electrónicos con datos personales es a través del uso de OneDrive. Este programa, aunque no contempla la opción de encriptar archivos electrónicos, permite controlar qué personas pueden acceder o editar los archivos compartidos. Para ello, se debe realizar el siguiente procedimiento:

Paso 1. Ingresar, mediante el programa OneDrive, a la carpeta o archivo que se desea compartir.

Paso 2. Dar clic secundario (botón derecho del ratón en la mayoría de los casos) y seleccionar la opción de Compartir.

Paso 3. Escribir los correos electrónicos de los destinatarios y seleccionar las personas que tendrán acceso al vínculo.

Paso 4. Determinar si se permitirá edición de los usuarios a los que se les comparte el vínculo en caso de archivos editables.

Paso 5. Dar clic en "Aplicar". La herramienta de OneDrive genera una liga que se podrá copiar y colocar en el correo electrónico requerido para dar conocimiento de a quien se le comparte el recurso.

Es importante aclarar que los usuarios deben estar migrados a Office365. En caso contrario, solicitar a la DGTI dicha migración a través de la mesa de servicios.

V. Conclusión

Esta guía es de carácter informativo y orientada a conseguir que la transmisión de datos personales se realice de manera segura. Son medidas básicas que garantizan, cuando menos, que la información no quede expuesta a personas ajenas al emisor y al destinatario.

Todos los usuarios son responsables de la información que generen, utilicen y transfieran, a través de los medios informáticos que utilicen, así como de implementar y supervisar los controles para protegerla durante su manejo considerando la clasificación y gestión de la información de acuerdo con sus atribuciones y/o funciones.

Dudas o comentarios dirigirse a:

Unidad General de Transparencia y Sistematización de la Información Judicial

Dirección de Protección de Datos Personales

Correo electrónico: datospersonales@mail.scjn.gob.mx

Teléfono: 55-4113-1000 Ext.5817

Suprema Corte
de Justicia de la Nación