Suprema Corte
de Justicia de la Nación

Catálogo de Medidas de Seguridad para los tratamientos de datos personales

UNIDAD GENERAL DE TRANSPARENCIA Y SISTEMATIZACIÓN
DE LA INFORMACIÓN JUDICIAL

I. Justificación

En términos de las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Suprema Corte de Justicia de la Nación (SCJN) es responsable de la protección y confidencialidad de los datos personales que recaba para realizar sus funciones u ofrecer sus servicios. Por tanto, tiene la obligación de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para ello.

La finalidad de las medidas de seguridad enfocadas especialmente en la protección de los datos personales es evitar cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado en las actividades cotidianas de las áreas administrativas que integran la SCJN y que pudieran afectar la confidencialidad de los mismos, dejando en estado de vulnerabilidad a sus titulares.

Para la elaboración del Catálogo de Medidas de Seguridad para los Tratamientos de Datos Personales de la Suprema Corte de Justicia de la Nación (CATÁLOGO–SCJN), la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTISJ) realizó un censo informativo con aquellas áreas involucradas en el tratamiento de los datos personales (Encuesta sobre análisis de riesgo y medidas de seguridad), con la finalidad de conocer dos aspectos:

i) El nivel de riesgo a que pudieran estar expuestos los datos personales.

ii) La naturaleza y alcances de las medidas de seguridad implementadas por las áreas que impactan de manera directa o indirecta en la protección de datos personales.

Asimismo, este CATÁLOGO–SCJN se construyó a partir de los parámetros normativos y buenas prácticas que se desprenden de la propia LGPDPPSO.

II. Políticas de seguridad en la Suprema Corte de Justicia de la Nación

De conformidad con los artículos 3, fracción XX y 31 de la LGPDPPSO, los sujetos obligados deben implementar diversas medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales.

La SCJN, por la propia naturaleza de sus funciones y previo a las disposiciones legales en materia de protección de datos personales, ha implementado diversos

mecanismos encaminados a la seguridad y protección de los datos personales que trata en el marco del ejercicio de sus atribuciones legales y reglamentarias.

Por ejemplo, las medidas de seguridad de carácter ***administrativo*** son aquellas relacionadas con la organización del sujeto obligado. Se refieren a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal en materia de protección de datos personales.

Al respecto, las áreas de la SCJN tienen la obligación de generar diversos documentos relacionados con dichas medidas de seguridad. Como ejemplo, se encuentran los Manuales de Operaciones Específicos en donde se describen los procesos, responsables y obligaciones respecto del tratamiento de datos personales; las políticas archivísticas; y, las políticas de capacitación en la materia.

Las medidas de seguridad de carácter ***físico*** son aquellas encaminadas a la protección del entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Algunas medidas previstas por la propia LGPDPPSO son las de prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; entre otros.

Sobre el particular, la SCJN cuenta con la Dirección General de Seguridad, misma que se ocupa de brindar y supervisar los servicios de seguridad a los servidores públicos, así como de preservar los bienes muebles e inmuebles de la misma; establecer, coordinar y mantener un sistema riguroso para el control de los ingresos en los módulos de acceso para el control y registro de la identificación oficial de los servidores públicos y usuarios de los servicios que son brindados en la SCJN; vigilar e inspeccionar de forma sistemática para fines de seguridad, los inmuebles ubicados en el Ciudad de México, así como los diversos inmuebles en el interior de la República, en todas sus áreas; entre otras.

Por último, las medidas de seguridad de carácter ***técnico*** son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Algunas medidas establecidas en la LGPDPPSO son las de prevenir el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; generar un esquema de privilegios; gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales, entre otras.

Sobre este tipo de medidas, la SCJN cuenta con la Dirección General de Tecnologías de la Información, que se encarga, entre otras cosas, de administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia; planear, diseñar, mantener y supervisar la operación de los sistemas de información y comunicación que requieran los órganos y áreas; proporcionar los servicios de mantenimiento a las redes, sistemas, equipo informático, comunicación y digitalización de los órganos y áreas de la SCJN y, en su caso, a otros órganos del Poder Judicial de la Federación; ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento.

Por lo anterior, es posible advertir que, en principio, la SCJN cuenta con medidas de seguridad generales de los tres tipos y acordes a los parámetros normativos de la protección de los datos personales; sin embargo, el CATÁLOGO–SCJN tiene como finalidad identificar las medidas de seguridad específicas que existen en cada una de las áreas administrativas en sus entornos cotidianos y encauzar la implementación de aquellas adicionales que se requieran para garantizar la efectiva protección de los datos personales.

III. Medidas de seguridad para los tratamientos de datos personales en la Suprema Corte de Justicia de la Nación

A partir de lo referido en los apartados anteriores y la información que se recabó a través del censo informativo, el CATÁLOGO–SCJN se integra de manera enunciativa por las siguientes medidas que las áreas habrán de implementar en función del nivel de riesgo de cada uno de sus tratamientos:

Medidas de seguridad administrativas

A. **Declaración de confidencialidad:** realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.

B. **Listado de personal:** elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre,

cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.

C. **Clasificación de los archivos físicos:** identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.

D. **Clasificación de los archivos electrónicos:** identificar y etiquetar las bases de datos en soporte electrónico con el nombre del Tratamiento de Datos Personales conforme al Inventario reportado por el área.

E. **Capacitación:** el personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.

F. **Bitácora de vulneraciones:** implementar un control informativo en donde se reporten los tipos de vulneraciones[1] con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la UGTSIJ para que tome las acciones pertinentes.

   Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.

G. **Depuración y borrado seguro del archivo físico:** Transferir y depurar el archivo físico de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.

H. **Depuración y borrado seguro del archivo electrónico:** borrar, de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo. Solicitar a Dirección General de Tecnologías de la Información que proporcione un programa para el borrado integral de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, para la depuración y borrado seguro de

[1] De conformidad con el artículo 38 de la LGPDPPSO, son: I) La pérdida o destrucción no autorizada; II) el robo, extravío o copia no autorizada; III) el uso, acceso o tratamiento no autorizado, o IV) el daño, alteración o modificación no autorizada.

las bases de datos electrónicas, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la UGTSIJ.

I. **Bitácora de consulta:** establecer una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.

J. **Responsable de seguridad:** designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.

K. **Transferencias:** realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.

Medidas de seguridad físicas

A. **Cuidado de los bienes informáticos:** Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por la Dirección General de Tecnologías de la Información, tampoco alterar el orden de los cables conectados.[2]

B. **Prevenir accesos no autorizados:** prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.

C. **No instalar equipos ajenos:** Abstenerse de instalar equipos de cómputo que no sean propiedad de la SCJN sin permiso de la Dirección General de Tecnologías de la Información. Los usuarios que requieran hacer uso de la red interna de SCJN deben usar solamente las direcciones IP asignadas por el área administrativa correspondiente. En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus. En el caso de encontrarse infectado el dispositivo, el usuario debe extraer inmediatamente sin consultar, modificar o copiar información alguna.

D. **Traslado de equipos de cómputo:** observar el procedimiento dispuesto por el Acuerdo General de Administración IV/2008, del dieciséis de mayo de dos mil ocho,

[2] Cada usuario será responsable del resguardo del equipo de cómputo que se le haya proporcionado para el desempeño de sus funciones, de conformidad con las necesidades propias del órgano de su adscripción.

del Comité de Archivo, Biblioteca e Informática, relativo al uso y aprovechamiento de los bienes y servicios informáticos de la Suprema Corte de Justicia de la Nación, para el traslado de equipos de cómputo fuera de las instalaciones de la SCJN.

E. **Archivero con candado:** Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado.

F. **Candados de seguridad para equipos de cómputo:** fijar con candados de seguridad los equipos de cómputo que contengan bases de datos personales.

G. **Zona de confidencialidad:** definir una zona de confidencialidad en donde se resguardarán los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado.

Medidas de seguridad técnicas

A. **Cuidado de la contraseña personal:** abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático de la SCJN.

B. **Actualización de contraseñas:** cambiar las contraseñas cada tres meses por lo menos, a efecto de evitar robo de identidad. En caso de olvido o sospecha de divulgación de una contraseña o mecanismo de autenticación, los usuarios deberán realizar el cambio de los mismos en los sistemas informáticos de la SCJN.

C. **Reportar fallas:** notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.

D. **No instalar softwares:** abstenerse de descargar en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.

E. **Contraseñas robustas:** construir contraseñas con rol de administrador de forma robusta, atendiendo a los siguientes criterios:

- Contar con una longitud mínima de 12 caracteres.
- Incluir, por lo menos, dos letras mayúsculas, dos letras minúsculas, dos símbolos especiales (punto, coma, guion, etcétera) y un número;

- Evitar el uso de palabras comunes o datos personales;
- Renovarlas de manera periódica;
- Las contraseñas no podrán repetirse en al menos 10 iteraciones;
- Almacenarlas de forma cifrada y en archivos electrónicos distintos en los que se almacenan datos de aplicaciones.

F. **Respaldo de información:** realizar respaldos de la información que resida en el equipo de cómputo asignado. La Dirección General de Tecnologías de la Información, a solicitud del usuario, asesorará y apoyará a los usuarios en el procedimiento para considerando las necesidades propias del área.

IV. Nivelación de las medidas de seguridad de acuerdo al nivel de riesgo

Las medidas de seguridad que deberán adoptarse deben tomar como referencia el nivel de riesgo latente que presenta cada tratamiento de datos personales.

La UGTSIJ, a través de la ***Encuesta sobre análisis de riesgo y medidas de seguridad***, identificó, en conjunto con las áreas de la SCJN, los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales. De la suma de estos riesgos fue posible calcular el nivel de riesgo latente en cada caso.

Los resultados fueron esquematizados de la siguiente manera:

Nivel de riesgo	Resultado de la encuesta
Bajo	3 a 5
Medio	6 a 8
Alto	9 en adelante

La combinación de estos resultados, con la naturaleza de cada medida de seguridad propuesta en el CATÁLOGO–SCJN, hace posible clasificar las medidas de seguridad que habrán de implementarse atendiendo el nivel de riesgo, lo cual se ilustra de la siguiente manera:

Medidas de seguridad / Niveles de riesgo latente	Administrativas	Físicas	Técnicas
Bajo	A-F	A-D	A-D
Medio	A-H	A-E	A-E
Alto	A-K	A-G	A-F

Es necesario recordar que estas medidas de seguridad son complementarias y refuerzan aquellas implementadas como política institucional de seguridad en la SCJN, coordinadas por las áreas competentes, entre ellas, la Dirección General de Seguridad y la Dirección General de Tecnologías de la Información.

Dudas o comentarios dirigirse a:

Unidad General de Transparencia y Sistematización de la Información Judicial

Correo electrónico:

datospersonales@mail.scjn.gob.mx

Suprema Corte de Justicia de la Nación