Unidad General
de Transparencia
y Sistematización de
la Información Judicial

Programa de protección de datos personales

Suprema Corte
de Justicia de la Nación

Presentación

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) establece la obligación para los sujetos obligados de adoptar mecanismos para cumplir con el principio de responsabilidad a través de la elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable (artículo 30, fracción II).

Por su parte, los Lineamientos Generales de Protección de Datos Personales para el Sector Público establecen que el responsable deberá elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua (artículo 47).

A partir de la publicación de estas disposiciones, la Unidad General de Trasparencia y Sistematización de la Información Judicial (UGTSIJ) identificó la ruta que debería trazarse para encaminar el cumplimiento institucional en la materia, partiendo de la premisa de que el ámbito de trabajo se limitaría, en un principio, a la parte administrativa de este Alto Tribunal, y puso a consideración del Comité de Transparencia una propuesta de política institucional con esa óptica.

En ese sentido, en la institución se aprobó el primer Documento de Seguridad 2019 que permitió conocer el estado de cosas, las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales. Asimismo, se implementó un primer Plan de Trabajo (2019-2022) cuyos objetivos fueron los de eliminar las brechas a través de la implementación de medidas de seguridad pendiente en cada uno de los tratamientos de datos personales y consolidar y preservar los niveles de protección de datos personales a través de mecanismos de monitoreo y revisión.

Eso permitió identificar los alcances de las obligaciones establecidas en la propia Ley General y adaptarlas a través de acciones, guías y recomendaciones de conformidad con la naturaleza de cada uno de los tratamientos de datos personales registrados.

Por tanto, el Programa de Protección de Datos Personales de la Suprema Corte de Justicia de la Nación (PPDP-SCJN) que aquí se desarrolla toma como referencia el camino recorrido en la institución con la certeza de los objetivos, responsabilidades y alcances que debe tener este tipo de documentos para la Suprema Corte de Justicia de la Nación. Asimismo, este Programa permite constituirse como el sistema de gestión que

establece el artículo 34 de la Ley General, en tanto identifica los elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Asimismo, cabe señalar que este sistema de gestión se basa en el que ha sugerido el INAI en el *Documento Orientador para la elaboración del Programa de Protección de Datos Personales*, publicado en agosto de 2018 como herramienta de facilitación y orientación para los Sujetos Obligados. Además, toma como referencia las Recomendaciones para la elaboración de *Políticas internas de gestión y tratamiento de datos personales* del INAI.

Este PPDP-SCJN podrá ser sometido a su revisión, ajuste o actualización por parte del Comité de Transparencia, cuando se produzcan modificaciones sustanciales a las obligaciones previstas en este Programa.

Glosario

Aviso de privacidad: documento a disposición del titular de forma física, electrónica o en cualquier formato generado por la SCJN, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Ciclo de vida: el ciclo de vida de los datos abarca todo el periodo en el que los datos existen en una organización, desde la obtención de los datos hasta su eliminación.

Datos personales: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificada cuando se acredita su identidad a través de cualquier información relacionada ella, por ejemplo, su nombre, teléfono, domicilio, fotografía, huellas dactilares o cualquier otro dato personal. Asimismo, será una persona identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Derechos ARCO: los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

- Acceso: Derecho del titular para acceder a sus datos personales que obren en posesión de la SCJN, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- Rectificación: Derecho del titular para solicitar a la SCJN la corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

- Cancelación: Derecho del titular para solicitar a la SCJN que sus datos personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.
- Oposición: Derecho del titular para solicitar a la SCJN, cuando ésta pretenda realizar el tratamiento de datos personales, que se abstenga de hacerlo en determinadas situaciones o para que cese el tratamiento.

Documento de seguridad: instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la SCJN para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Inventario de Tratamientos: documento donde se relacionan los tratamientos de datos personales que realizan las áreas u órganos de la SCJ, con la información básica que los describe.

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Persona enlace de seguridad de datos personales: persona servidora pública designada por su área/órgano para coordinar y auxiliar en la implementación de las medidas de seguridad establecidas en el Documento de Seguridad.

Persona titular: la persona a quien corresponden los datos personales.

Portal: Portal de Protección de Datos Personales de la Suprema Corte de Justicia de la Nación.

PPDP-SCJN: el presente Programa de Protección de Datos Personales de la Suprema Corte de Justicia de la Nación.

Responsable: la SCJN a través de las áreas y órganos que se le adscriben, en tanto que deciden sobre el tratamiento de datos personales acorde a las facultades y atribuciones conferidas en los ordenamientos normativos.

ROMA: Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación.

SCJN: Suprema Corte de Justicia de la Nación.

SG-PDP: Sistema de Gestión para la Protección de Datos Personales de la Suprema Corte de Justicia de la Nación.

Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

UGTSIJ: Unidad General de Transparencia y Sistematización de la Información Judicial.

Objetivos del Programa

El presente programa tiene como objetivos los siguientes:

1. Integrar las acciones, referencias y documentos que constituyen la política de protección de datos personales en la Suprema Corte de Justicia de la Nación;
2. Establecer el marco de referencia y de trabajo necesarios para el debido tratamiento y protección de datos personales en posesión de las áreas y órganos administrativos;
3. Cumplir con las obligaciones que establece la Ley General y los Lineamientos Generales, así como la normatividad que derive de los mismos y que resulte aplicable a la SCJN;
4. Promover la adopción de mejores prácticas en la materia, incluyendo la perspectiva de la protección de datos personales en todos los proyectos institucionales que implique su tratamiento; y
5. Implementar el programa de manera integral en la Suprema Corte de Justicia de la Nación.

Alcances del Programa

El PPDP-SCJN es de observancia obligatoria para todas las áreas y órganos previstos en el artículo 2, fracciones I y IV, del ROMA que realicen tratamiento de datos personales en ejercicio de sus atribuciones y funciones.

Las áreas y órganos que, al día de la elaboración de esta versión del PPDP-SCJN, tratan datos personales, pueden consultarse en el Inventario de Tratamientos: https://datos-personales.scjn.gob.mx/medidas-de-seguridad/nuevos-tratamientos.

Todos los proyectos o actividades de estos que impliquen tratamientos de datos personales deberán observar —desde su planeación— los principios, deberes y medidas de seguridad en la materia.

Por tanto, las áreas y órganos administrativos deberán prever la disposición de recursos humanos, materiales y financieros para la consecución de estos fines.

Responsabilidades del Programa

Para la aprobación, interpretación, orientación y aplicación de las diversas acciones previstas en el presente PPDP-SCJN, las responsabilidades se identifican en diversos niveles.

Comité de Transparencia

1. Aprueba el PPDP-SCJN, así como su modificación y actualización.
2. Propone cambios y mejoras, a partir de los elementos que le informe la UGTSIJ.

Unidad General de Transparencia y Sistematización de la Información Judicial

1. Propone al Comité de Transparencia el PPDP-SCJN, así como sus modificaciones y actualización.
2. Coordina su aplicación en las áreas y órganos administrativos.
3. Difunde su contenido.
4. Orienta a las áreas y órganos administrativos en su implementación.
5. Da seguimiento a su implementación por parte de las áreas y órganos, a fin de proponer medidas preventivas o correctivas para el debido tratamiento de los datos personales.
6. Informa al Comité de Transparencia sobre los avances, estado y resultados de la implementación del PPDP-SCJN.

Áreas y órganos administrativos

1. Aplican las acciones en sus proyectos y/o actividades que impliquen tratamiento de datos personales.
2. Cumplen con los principios y deberes en sus tratamientos registrados.
3. Implementan las medidas de seguridad recomendadas para la protección de datos personales en su posesión.

Enlaces de seguridad de datos personales

1. Difunden, entre las personas servidoras públicas que tratan datos personales adscritas a su área u órgano, las recomendaciones, insumos y documentos en el marco del programa.
2. Coordinan la implementación del PPDP-SCJN al interior de su área u órgano.
3. Fungen como enlace con la UGTSIJ para la coordinación y seguimiento de la implementación del PPDP-SCJN.

Política de Gestión de Datos Personales

La Ley General establece la obligación para los responsables de crear políticas internas para la gestión y tratamiento de los datos personales, los cuáles deberán tomar en cuenta el contexto del tratamiento y el ciclo de vida de los datos personales (Artículo 33, fracción I). Asimismo, considera que se debe garantizar que sus políticas, programas, servicios o sistemas que implique tratamiento de datos personales, cumplan por defecto con las disposiciones de la Ley General (artículo 30, fracción VIII).

Esto debe considerarse de manera integral, en el ciclo de vida de los tratamientos de datos personales de la institución. El ciclo de vida de los datos personales es el periodo durante el cual el responsable tiene bajo su posesión los datos personales, desde la obtención y el uso, hasta la supresión respectiva. Durante ese ciclo es necesario observar los principios y deberes para garantizar un tratamiento adecuado, adoptar las medidas de seguridad recomendadas y atender las disposiciones administrativas para el adecuado manejo de los archivos que los contengan.

En ese sentido, todos los tratamientos de datos personales deben cumplir con los principios y deberes previstos en la Ley General a lo largo del ciclo de vida de los datos personales, esto es, desde su obtención hasta su eliminación, pasando por la etapa de utilización de los datos personales, de conformidad con lo siguiente.

ETAPA 1. Obtención de los datos personales y planeación del proyecto

Durante la etapa de obtención de los datos personales y planeación de cualquier proyecto o actividad que implique tratamiento de datos personales, se debe cumplir con lo siguiente:

I. **Principio de licitud:** el tratamiento debe estar justificado por finalidades que estén previstas dentro de las atribuciones que la normativa confiere al área u órgano. En ese sentido, las áreas y órganos responsables del tratamiento deben responder la siguiente pregunta:

- ¿El tratamiento de datos se justifica en sus atribuciones previstas en el ROMA o la normativa que regula su actuación?

  Nota: De ser así, en el Inventario de Tratamientos se debe registrar el fundamento normativo que faculta al área u órgano para dicho tratamiento y este fundamento se deberá informar en el aviso de privacidad respectivo.

II. **Principio de proporcionalidad:** se deben tratar únicamente los datos personales que resulten relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. Por tanto, las áreas y órganos responsables deben verificar las siguientes preguntas:

- ¿Resulta necesario recabar datos personales para llevar a cabo la actividad?
- ¿Puedo disociar la información de tal forma que no se identifiquen las personas?
- ¿Recabo los datos necesarios e indispensables para llevar a cabo la actividad?
- ¿Puedo recabar menos datos personales de los planeados para llevar a cabo la actividad?

  Nota: En caso de recabar datos personales, éstos se deben enlistar en el tratamiento que se registre en el inventario, con la finalidad de conocer e informar el alcance de este.

III. **Principio de información:** se debe informar a las personas titulares de los datos, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que puedan tomar decisiones informadas al respecto. Para ello, se debe contar con el aviso de privacidad para ponerse a disposición

previo a la obtención de los datos personales. Por lo anterior, se debe asegurar lo siguiente:

- ¿El proyecto o actividad cuenta con su aviso de privacidad previo a su implementación?

  Nota: El aviso de privacidad es el mecanismo para cumplir con el principio de información y se debe tener listo antes de que inicien las actividades.

IV. Principio de consentimiento: los tratamientos que no actualicen los supuestos de excepción previstos en el artículo 22 de la Ley General se deberá solicitar el consentimiento del titular, en la modalidad que corresponda, esto es tácito, expreso o expreso por escrito, de conformidad con lo previsto en los artículos 20 y 21 de la Ley General. El consentimiento se deberá solicitar previo al tratamiento y quedar acreditado en el documento que resulte pertinente de conformidad con las características del tratamiento, por ejemplo, en el aviso de privacidad, un formulario, en un contrato, entre otros. En ese sentido, es importante verificar:

- ¿El tratamiento actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General?
- ¿Qué tipo de consentimiento se requiere?
- ¿En el procedimiento correspondiente se prevé la obtención del consentimiento?

  Nota: Si tengo la obligación de recabar el consentimiento, me debo asegurar que el aviso de privacidad informe sobre las finalidades que requieren el consentimiento, así como los mecanismos disponibles para otorgarlo o no. Si es tácito, que la persona titular tenga la posibilidad de negarse al tratamiento a través del aviso de privacidad; si es expreso, que puede manifestar su consentimiento, generalmente, a través de nombre y firma.

V. Deber de seguridad: implica que para todo tipo de tratamiento se deberán establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permita protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad. Las medidas que se han adoptado para los tratamientos de la Suprema Corte de Justicia de la Nación se encuentran en el Documento de Seguridad. Asimismo, en el SG-PDP se deben

reportar su implementación por cada tratamiento, por tanto, hay que verificar lo siguiente:

- ¿Implemento las medidas de seguridad para la protección de los datos personales aprobadas en el Documento de Seguridad que están bajo mi custodia?

  Nota: Puedes conocer el Catálogo de Medidas de Seguridad en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Catálogo%20de%20Medidas%20de%20Seguridad%20%282%29.pdf

  Este deber aplica a lo largo de todo el ciclo de vida de los datos personales.

VI. Deber de confidencialidad: este deber implica que se deben establecer los controles o mecanismos que tengan por objeto prevenir la difusión de los datos personales a personas no autorizadas o legitimadas. En ese sentido, se debe asegurar lo siguiente:

- ¿El listado de personas servidoras públicas que intervienen en el tratamiento de datos se encuentra actualizado en el SG-PDP?
- ¿Me aseguro de que las personas servidoras públicas conozcan sus obligaciones con relación a la protección de datos personales?
- ¿Cumplo con las medidas de seguridad que corresponden al tratamiento de datos personales que realizo?

  Nota: solicita la capacitación que requiera el personal del área u órgano a la UGTSIJ. Para conocer las recomendaciones relacionadas con la protección de los datos personales, se encuentran los recursos y medidas implementadas publicadas en el Portal: https://datos-personales.scjn.gob.mx/medidas-de-seguridad/Recursos-y-medidas-implementadas

  Este deber aplica a lo largo de todo el ciclo de vida de los datos personales.

Etapa 2. Utilización de los datos personales o implementación del proyecto

Una vez que se obtuvieron los datos personales o se pone en marcha el proyecto, es importante cerciorarse de que se cumplan con otros principios y deberes que garantizan la confidencialidad de la información y debido tratamiento:

I. Principio de finalidad: las finalidades para las cuales se recaban y tratan los datos personales deben ser concretas, lícitas, explícitas y legítimas, además de estar justificadas por las atribuciones que la normativa aplicable le confiere al área u órga-

no. Asimismo, los datos personales deberán ser tratados para las finalidades informadas en el aviso de privacidad o consentidas por el titular. De tal manera que, las áreas y órganos deben responder las siguientes preguntas:

- ¿La finalidad es concreta, lícita, explícita y legítima?
- ¿Se informa la finalidad de manera clara en el aviso de privacidad?
- ¿El tratamiento se limita para las finalidades informadas en el aviso de privacidad?

  Nota: Las finalidades deben identificarse en los avisos de privacidad para que las personas titulares tomen decisiones informadas y en el tratamiento que se registre.

II. Principio de calidad: el responsable cumple con este principio cuando se mantienen exactos, completos, correctos y actualizados los datos personales. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario. En ese sentido, es importante verificar:

- ¿Las fuentes de obtención de los datos personales son confiables y las adecuadas?
- ¿Cuándo tengo conocimiento —a través de una fuente autorizada o confiable— del cambio en el registro de algún dato personal, lo actualizo o corrijo en el archivo o base de datos que corresponda?

III. Principio de lealtad: este principio implica que los datos personales no se recaben por medios engañoso o fraudulentos y que se debe privilegiar la protección de los intereses de la persona titular y su expectativa razonable de privacidad. Es decir, es importante acreditar lo siguiente:

- ¿Respeto la finalidad por la que recabé los datos de la persona titular?
- ¿Me cercioro de que los datos personales se encuentran protegidos?

  Nota: Cuidar los datos personales como si fueran mis datos personales, te brinda una perspectiva de cómo tratar esa información.

Etapa 3. Eliminación de los datos personales

Una vez que los datos personales han dejado de cumplir con su finalidad y/o se cumplió con el periodo de conservación que establecen los instrumentos archivísticos, se de-

ben observar las pautas para asegurarse que, en esta última etapa del ciclo de vida, no se vulnerará la confidencialidad de esa información.

I. Principio de calidad: en esta etapa, este principio implica que los datos personales deben atender los plazos de conservación establecidos en los instrumentos de consulta archivística, por lo que, una vez concluidos, deberán ser eliminados. Esto implica que los responsables de la información deberán verificar lo siguiente:

- ¿Conozco el plazo de conservación a que están sujetos los datos personales de los tratamientos que soy responsable?
- ¿Suprimo y doy de baja los datos personales de todo archivo físico o electrónico cuando éstos cumplen su plazo de conservación?

Nota: Para asegurar la eliminación de los datos personales es importante respetar los plazos de conservación de la serie archivística a la que pertenecen y solicitar orientación al CDAACL.

Sistema de Gestión para la Protección de Datos Personales (SG-PDP)

La UGTSIJ diseñó e implementó un sistema informático para materializar un Sistema de Gestión para la Protección de los Datos Personales (SG–PDP) que permite a las áreas/órganos emprender acciones y consultar insumos en materia de protección de datos personales en un solo espacio digital, y autogestionar la implementación, operación, actualización, monitoreo y revisión de los principios y las medidas de seguridad de los tratamientos bajo su responsabilidad.

El SG–PDP pretende consolidar el nivel de protección de los datos personales y materializar, de manera innovadora y bajo un esquema de mejores prácticas, el sistema de gestión al que refiere el artículo 34 Ley General.

El sistema se diseñó como un sitio web (con acceso desde intranet), cuya funcionalidad está compuesta principalmente por formularios con campos de información que pueden ser llenados por los usuarios del sistema. La razón del desarrollo bajo esta funcionalidad es facilitar el acceso y mejorar la experiencia de las personas usuarias, pues evita descargar y/o instalar aplicaciones, y la conexión a internet es suficiente para ingresar a dicho sistema.

El tratamiento debe registrarse a través del SG-PDP. Esto permite cumplir con varias obligaciones en la materia:

- Contar con un Inventario de Tratamientos completo y actualizado.
- En el SG-PDP se deben relacionar las personas y las funciones que intervendrán en el tratamiento de datos personales.
- El SG-PDP permite identificar si el tratamiento requiere del consentimiento previo de las personas para tratar sus datos personales.
- El tratamiento debe relacionarse con la clave archivística a la que correspondan los archivos para conocer el plazo de conservación a que estarán sujetos los datos personales.
- El SG-PDP permite contar con los formatos de aviso de privacidad integral y simplificado, de conformidad con la información del tratamiento.
- También se puede conocer el nivel de riesgo del tratamiento, relacionado con la naturaleza de los datos que se recaban, dónde se almacenan y quién accede a los mismos.
- Por último, el SG-PDP permite identificar cuáles son las medidas de seguridad con que cuenta el tratamiento de datos personales desde su inicio y cuáles son las que quedarían pendientes de implementar.

Así, a través del SG-PDP las áreas y órganos que tratan datos personales pueden actualizar y consultar la siguiente información:

- Inventario de tratamientos: las áreas reportan la información de cada uno de sus tratamientos de datos personales; la información que la compone se desarrolla en el siguiente apartado.
- Avisos de privacidad: el SG-PDP genera avisos de privacidad de manera automática con la información que se reporta en cada uno de los tratamientos.
- Nivel de riesgo: el SG-PDP mide el nivel de riesgo que corresponde a cada uno de los tratamientos (bajo, medio o alto), de conformidad con las variables que se establecieron en la Metodología.
- Análisis de brecha: las áreas seleccionan las medidas de seguridad que se han implementado en cada uno de los tratamientos, de acuerdo con el Catálogo de Medidas de Seguridad; por tanto, se identifican aquellas que hacen falta implementarse.
- Documentos relevantes: a través de dicho sistema se pone a disposición de las áreas y órganos el Documento de Seguridad vigente, el Plan de Trabajo en la materia vigente, los informes sobre la materia y el inventario de tratamientos vigente.
- Capacitación: el SG-PDP se configurará como un medio para poner a disposición de todas las personas que tratan datos personales, insumos de capacitación como cuestionarios de evaluación, guías, cápsulas, infografías.
- Mecanismos de monitoreo y revisión: este espacio también servirá como un medio para implementar estos mecanismos para verificar el nivel de cumplimiento de los principios y deberes.

Inventario de Tratamientos

El Inventario de Tratamientos de Datos Personales (Inventario) es el documento donde se relacionan los tratamientos de datos personales que realizan las áreas u órganos de la SCJ, con la información básica que los describe, contemplado en los artículos 33, fracción III y 35, fracción I, de la Ley General como un elemento del Documento de Seguridad.

El Inventario se actualiza permanentemente de conformidad con la información o los cambios que las propias áreas responsables realizan en el SG-PDP en cada uno de los elementos de los tratamientos de datos personales o, en su caso, por su registro inicial, fusión o eliminación. Se publica semestralmente la versión actualizada del propio Inventario a través de nuestro Portal de Datos Personales.

Los elementos que actualmente se identifican en el Inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa.
- Nombre y clave del tratamiento.
- Finalidad.
- Fundamento normativo.
- Datos personales que se recaban.
- Tipo de consentimiento.
- Forma de obtención de los datos personales.
- Tipo de soporte en el que se almacena la base de datos personales.
- Ubicación del tratamiento.
- Referencia documental conforme al Catálogo de Disposición Documental vigente.
- Información sobre transferencias de datos personales.
- Plazo de conservación.

El Inventario identifica, a través de una clave alfabética, cada una de las áreas responsables que tratan datos personales y con un número alfanumérico los tratamientos bajo su responsabilidad (por ejemplo, área: A; tratamientos: A1, A2, A3, así consecutivamente).

A través de los elementos que lo componen, el inventario permite identificar el cumplimiento de varios principios en la materia por parte de las áreas y órganos que lo actualizan: finalidad, licitud, proporcionalidad, consentimiento, calidad (conservación) y responsabilidad.

En un principio se contó con el registro de 21 áreas y/u órganos que tratan datos personales, con un total de 80 tratamientos registrados. La última actualización de noviembre 2022 cuenta con 24 áreas/órganos administrativos de este Alto Tribunal, con un total de 81 tratamientos de datos personales.

Sobre todos estos tratamientos deben implementarse las pautas previstas en este PPDP-SCJN. El Inventario puede consultarse de manera actualizada en el siguiente enlace: https://datos-personales.scjn.gob.mx/medidas-de-seguridad/nuevos-tratamientos

Avisos de Privacidad

El aviso de privacidad es el documento a disposición de la persona titular de los datos personales de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos de su tratamiento.

De acuerdo con los artículos 18, 26 y 27 de la Ley General, cada tratamiento de datos personales debe contar con su aviso de privacidad integral y uno simplificado. Estos avisos deben hacerse del conocimiento de las personas de manera previa a que se recaben sus datos personales para que esté en posibilidad de informarse sobre la naturaleza y el alcance del tratamiento a que se someterán sus datos y decida de manera informada sobre el mismo.

Los avisos de privacidad son generados de manera automática por el SG-PDP para cada uno de los tratamientos de datos personales registrado. El aviso de privacidad simplificado debe ponerse a disposición por parte de las áreas y órganos a las personas titulares cuando los datos se recaban de manera física en presencia de estos. El aviso de privacidad integral se debe colocar para su consulta cuando los datos se recaban de manera electrónica o formularios que permiten poner a disposición su enlace electrónico.

Además de cumplir con el principio de información, a través de los avisos de privacidad las áreas y órganos recaban el consentimiento de las personas titulares cuando se tiene la obligación de hacerlo.

Las áreas y órganos son responsables de generar y actualizar sus propios avisos de privacidad, a través de la carga de información que se realiza en el SG-PDP.

Los avisos integrales se pueden consultar en el repositorio: https://datos-personales.scjn.gob.mx/avisos-de-privacidad

Medidas de Seguridad

En términos de las disposiciones de la Ley General, 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 y órganos administrativos que integran la SCJN y que pudieran afectar la confidencialidad de los mismos, dejando en estado de vulnerabilidad a sus titulares.

Es importante decir que la política de seguridad en general, y la política de seguridad de la información en particular, de la Suprema Corte de Justicia de la Nación, se tienen implementadas y desarrolladas previo a las disposiciones legales en materia de protección de datos personales, en el marco del ejercicio de sus atribuciones constitucionales y legales.

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; la política de control de riesgos con perspectiva de ética pública; y, las políticas de capacitación en la materia. Para ello se cuenta con las áreas de la Dirección General de Planeación, Seguimiento e Innovación; el Centro de Documentación y Análisis, Archivo y Compilación de Leyes; y la Dirección General de Recursos Humanos.

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 Ley General 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 a los edificios de 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 Ley General 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.

En ese sentido, la UGTSIJ elaboró un Catálogo de Medidas de Seguridad complementarias a las que existen en la institución, cuya finalidad es garantizar, en lo específico, la efectiva protección de los datos personales y evitar cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado en las actividades cotidianas de las áreas y órganos administrativos.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS		
Tipo de medida	**Descripción**	**Insumo o área responsable**
Declaración de confidencialidad	Resguardar las declaratorias que han sido firmadas y puestas 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.	Declaratoria de confidencialidad

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS		
Tipo de medida	**Descripción**	**Insumo o área responsable**
Listado de personal que interviene en el tratamiento de datos	Contar con la relación actualizada de las personas que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones que realiza en el tratamiento, formato en que se realiza y fundamento normativo, por cada tratamiento.	Listado de personal SCJN
Clasificación de los archivos físicos	Identificar la clave archivística a la que pertenece el tratamiento de datos personales y observar el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.	Guía para la conservación y eliminación de documentos y expedientes que contienen datos personales Inventario de tratamientos de datos personales
Clasificación de los archivos electrónicos	Identificar la clave archivística a la que pertenecen los tratamientos en formato electrónico e integrarlos al expediente electrónico correspondiente, conforme a la Guía para la conservación y eliminación de documentos y expedientes que contienen datos personales.	
Depuración y borrado seguro del archivo físico	Transferir y depurar los documentos y archivos electrónicos que contengan datos personales de manera periódica, conforme a los plazos de conservación y parámetros dispuestos en el Catálogo de Disposición Documental.	
Depuración y borrado seguro del archivo electrónico	Implementar un programa de borrado –seguro y permanente– de 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. Una posibilidad es el borrado integral de la información o, en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la UGTSIJ.	
Capacitación	Haber asistido a los cursos y consultado los insumos de capacitación implementados por el Comité de Transparencia en los Programas Anuales de Capacitación correspondientes.	Capacitación
Bitácora de vulneraciones	Atender el Instructivo para registrar y reportar vulneraciones de datos personales en caso de que haya ocurrido alguna vulneración.	Instructivo para registrar y reportar vulneraciones de datos personales

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS		
Tipo de medida	**Descripción**	**Insumo o área responsable**
Bitácora de consulta	En caso de contar con tratamientos cuyo nivel de riesgo es alto y, además, contienen datos personales sensibles y se alberguen en algún sistema informático, haber solicitado a la DGTI la implementación de la Bitácora de Consulta, bajo los estándares recomendados.	DGTI
Enlace de seguridad	Haber designado un enlace de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.	UGTSIJ
Transferencias	Se realizan transmisiones seguras de datos personales cuyo tratamiento está bajo su responsabilidad, implementando medidas de seguridad básicas de carácter administrativo y tecnológico, conforme la Guía para la transmisión segura de datos personales.	Guía para la transmisión segura de datos personales

MEDIDAS DE SEGURIDAD FÍSICAS		
Tipo de medida	**Descripción**	**Insumo**
Cuidado de los bienes informáticos	Se protegen los bienes informáticos de conformidad con las recomendaciones de la Guía de seguridad informática para la protección de datos personales.	Guía de seguridad informática para la protección de datos personales
No instalar equipos ajenos	No se instalan dispositivos no autorizados por la Dirección General de Tecnologías de la Información, observando las medidas de la Guía de seguridad informática para la protección de datos personales.	
Archivero con candado	Se resguardan 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.	DGRM
Candados de seguridad para equipos de cómputo	Fijar con candados de seguridad los equipos de cómputo que contengan bases de datos personales.	DGTI
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.	DGS
Traslado de equipos de cómputo	Se adoptan las medidas adecuadas para el traslado de equipos de cómputo fuera de las instalaciones de la SCJN, de conformidad con la Guía de seguridad informática para la protección de datos personales.	Guía de seguridad informática para la protección de datos personales

MEDIDAS DE SEGURIDAD FÍSICAS		
Tipo de medida	**Descripción**	**Insumo**
Zona de confidencialidad	Se encuentra definida una zona de confidencialidad en donde se resguardan los archivos físicos o equipos de cómputo que contengan las bases de datos de riesgo alto, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado.	UGTSIJ y DGIF

MEDIDAS DE SEGURIDAD TÉCNICAS		
Tipo de medida	**Descripción**	**Insumo**
Cuidado de la contraseña personal	Se cuidan correctamente las contraseñas personales de la red institucional, observando las recomendaciones de la Guía de seguridad informática para la protección de datos personales.	Guía de seguridad informática para la protección de datos personales
Actualización de contraseñas	Se mantienen actualizadas las contraseñas de autenticación en un lapso no mayor a 90 días.	
Reportar fallas	Notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.	
No instalar softwares	No se descargan ni instalan en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia, no autorizados por la Dirección General de Tecnologías de la Información, observando las medidas de la Guía de seguridad informática para la protección de datos personales.	
Contraseñas robustas	Se atienden las recomendaciones de la Guía de seguridad informática para la protección de datos personales, para la creación de contraseñas robustas y seguras.	
Respaldo de información	Se realizan respaldos de información de manera periódica para garantizar que la información almacenada en los equipos de cómputo no se afecte con alguna falla y esto se traduzca, a su vez, en una vulneración de la información, particularmente de los datos personales (pérdida o destrucción no autorizada).	

En la medida que el Catálogo referido se cumpla y se implemente para la mayoría de los tratamientos de datos personales, resulta relevante para la institución el diseño y elaboración de nuevas medidas de seguridad especializadas en la protección de datos personales, que respondan a necesidades particulares, con la colaboración de áreas especializadas en tecnologías, seguridad, archivos, entre otras.

Es importante decir que el Catálogo forma parte esencial del Documento de Seguridad–2023 y que incluso, se prevé su actualización en el marco del plan de trabajo del propio documento.

Documento de Seguridad 2023

El Documento de Seguridad es un instrumento que permite a los sujetos obligados conocer el estado de cosas, las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales. La Ley General establece la información básica que deberá contener dicho documento (artículo 35).

El Documento de Seguridad–2023, se compone de los siguientes elementos:

1. Inventario de tratamientos de datos personales.
2. Listado de personas que intervienen en los tratamientos de datos personales.
3. Análisis de riesgo.
4. Análisis de brecha.
5. Plan de trabajo 2023–2026.
6. Mecanismos de monitoreo y revisión.
7. Capacitación.

Este documento constituye una hoja de ruta que permite transitar sobre parámetros objetivos y realidades específicas para implementar las medidas encaminadas a la protección de los datos personales de la SCJN, definir los criterios, controles y programas de seguimiento y supervisar su debido cumplimiento en el ámbito de la información de carácter administrativo.

Los propósitos fundamentales de este Documento de Seguridad–2023 son:

1. Fortalecer la política institucional en la materia que ha sido implementada a lo largo de estos años.
2. Diseñar e implementar nuevas herramientas y medidas de seguridad que permitan profundizar en el cuidado de los datos personales.

Como se advierte, existe una clara relación entre los elementos del Documento de Seguridad y el PPDP-SCJN. Esto es así, en virtud de que el primero es un documento necesario para tener el mapa completo y planear la implementación de un programa con

alcances reales. Es decir, el Documento de Seguridad es la base de la ejecución de los pasos de la implementación del PPDP-SCJN.

Para síntesis del presente documento, no se reproduce el contenido del referido Documento de Seguridad y su consulta puede realizarse a través del enlace.

Revisiones y auditorías

De conformidad con el Plan de trabajo en materia de protección de datos personales (2023-2026), que forma parte del Documento de Seguridad–2023, se prevén mecanismos de monitoreo y revisión que tienen como objetivo fundamental preservar el nivel de cumplimiento y protección conseguido en la implementación de las medidas de seguridad, además de la mejora de los procesos en el tratamiento de los datos personales (artículo 35, fracción VI de la Ley General).

Al respecto, la Ley General menciona que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales (artículo 33, fracción VII).

Por lo anterior, se proponen diversas acciones relacionadas con el monitoreo y la revisión del cumplimiento de los principios y deberes en materia de protección de datos personales, que a continuación se desarrollan.

I. **Evaluación interna de cumplimiento.**

   Se propone generar una estrategia de revisión del cumplimiento de principios y deberes en materia de protección de datos personales. Asimismo, se cuenta con la Evaluación interna sobre la gestión de las solicitudes ARCO, con la finalidad de mejorar la calidad de la atención e identificar áreas de oportunidad en su trámite.

II. **Cuestionarios de monitoreo.**

   Los cuestionarios de monitoreo tienen como propósito evaluar el nivel de conocimiento e involucramiento del personal de este Alto Tribunal que interviene en el tratamiento de datos personales en torno a los conceptos y temas en la materia. Hasta el momento se han implementado cuatro cuestionarios, tres de ellos realizados a todas las personas que tratan datos personales y uno a las personas enlaces de seguridad designadas por cada áreas u órgano.

Acciones de mejora continua del Programa

El proceso de revisión y mejora continua permitirá verificar que los parámetros establecidos en la Ley General y en los Lineamientos Generales, en el PPDP-SCJN y en el Documento de Seguridad–2023 y demás normatividad aplicable de la que deriven obligaciones en materia de protección de datos personales se cumplan estrictamente o permitan realizar los ajustes necesarios para su cumplimiento y perfeccionamiento.

En ese sentido, la UGTSIJ —a través de la implementación mecanismos de monitoreo y revisión, la actualización de los elementos del Documento de Seguridad–2023 o a través de la rendición de informes sobre la materia— advertirá los puntos de mejora en la materia de protección de datos personales y realizará la recomendación que estime pertinente para la actualización del PPDP-SCJN.

Sanciones

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar un exhorto a la unidad administrativa correspondiente para que ésta lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las y los servidores públicos que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la Ley General serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley General de Datos Personales;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General de Datos Personales, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General de Datos Personales; No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General de Datos Personales;

VIII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General de Datos Personales;

IX. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en Ley General de Datos Personales;

X. Obstruir los actos de verificación de la autoridad;

XI. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General de Datos Personales;

XII. No acatar las resoluciones emitidas por el Instituto, y

XIII. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control, contraloría o instancia equivalente y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo de conformidad con la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia y la UGTSIJ tomarán las medidas necesarias para que los servidores públicos de la SCJN conozcan esta información.

Dudas o comentarios dirigirse a:

Unidad General de Transparencia y Sistematización de la Información Judicial

Correo electrónico:

datospersonales@scjn.gob.mx

Suprema Corte
de Justicia de la Nación