Suprema Corte
de Justicia de la Nación

Documento de seguridad, aproximaciones institucionales

Suprema Corte de Justicia de la Nación

Unidad General de Transparencia y
Sistematización de la Información Judicial

Índice

I. Presentación

A partir de la reforma constitucional de 2009, la protección de datos personales quedó establecida como un derecho fundamental en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que reconoce que toda persona tiene derecho a la protección, y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales.

Posteriormente, la reforma constitucional de 2014 en materia de transparencia fortaleció los mecanismos de resguardo y estableció una directriz clara en el sentido de que todos los sujetos obligados deben garantizar medidas de seguridad adecuadas para la protección de los datos personales que poseen. En ese sentido, se otorgaron facultades al Congreso de la Unión para materializar el contenido de la reforma a través de leyes y así otorgarle "forma, alcance y sentido."[1]

Derivado de esta reforma constitucional, en enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados. En este nuevo esquema se reconoce a la Suprema Corte de Justicia de la Nación (SCJN) como sujeto obligado para cumplir con los deberes reconocidos por dicha ley.

La LGPDPPSO prevé la necesidad de realizar diversas actividades interrelacionadas para establecer y mantener medidas de seguridad encaminadas a la protección de los datos personales. Entre ellas destacan i) la

[1] Reforma en materia de transparencia". Gobierno de la República. https://www.gob.mx/cms/uploads/attachment/file/66464/13_Transparencia.pdf

creación de políticas internas para la gestión y tratamiento de datos personales; ii) la definición de funciones y obligaciones del personal involucrado en el tratamiento; iii) la elaboración de un inventario de datos personales y de los sistemas de tratamiento; iv) la realización de un análisis de riesgo considerando amenazas y vulnerabilidades existentes y recursos para su tratamiento; v) la realización de un análisis de brecha que compare medidas de seguridad, así como la elaboración de un plan de trabajo para implementar las faltantes; vi) el monitoreo y revisión de las medidas de seguridad; y, vii) la capacitación en la materia (artículo 33).

Además, la propia legislación establece la necesidad de que las medidas de seguridad se encuentren debidamente documentadas y, en particular, prevé la elaboración de un *documento de seguridad* (artículos 34 y 35).

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. En ese sentido, la LGPDPPSO establece la información básica que deberá contener dicho documento (artículo 35):

- Inventario de datos personales y de los sistemas de tratamiento
- Funciones y obligaciones de las personas que tratan los datos personales
- Análisis de riesgo
- Análisis de brecha
- Plan de trabajo
- Mecanismos de monitoreo y revisión de las medidas de seguridad
- Programa general de capacitación

Finalmente, la legislación establece como una de las figuras responsables en materia de protección de datos personales al Comité de Transparencia,

refiriéndole incluso como la autoridad máxima en ese renglón (artículo 83). Respecto de sus atribuciones, reconoce un par relacionadas con el establecimiento y supervisión de la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la propia LGPDPPSO, así como la supervisión, en coordinación con las áreas o unidades administrativas competentes, del cumplimiento de las medidas, controles y acciones previstas en el *documento de seguridad* (artículo 84 fracciones IV y V).

A partir de lo anterior, este documento elaborado por la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTSIJ) es una aproximación institucional para la definición de políticas en materia de protección de datos personales, particularmente encaminadas a la aprobación del *documento de seguridad* por parte del Comité de Transparencia.

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.

II. Acciones institucionales

Ante este escenario, la UGTSIJ coordinó los esfuerzos de todas las áreas administrativas del Alto Tribunal y desarrolló elementos indispensables para integrar *el documento de seguridad*, lo que derivó en la elaboración de los inventarios y análisis (riesgo y brecha), así como en la aproximación a ciertos elementos para aprobar otros documentos como el plan de trabajo y los mecanismos de monitoreo.

Ello implicó un trabajo transversal a lo largo de varios meses, así como diversas acciones de diseño, sensibilización, capacitación, análisis,

retroalimentación, evaluación, recopilación y sistematización de información, datos y medidas de seguridad institucionales.

A continuación se ofrecen los detalles más relevantes de cada una de estas actividades, las cuales derivaron en aproximaciones conceptuales, metodologías de trabajo y resultados tangibles para la toma de decisiones del Comité de Transparencia de la SCJN.

1) Identificación de obligaciones, *primera etapa*

La UGTSIJ identificó las obligaciones emanadas de la LGPDPPSO y advirtió diversas rutas para su cumplimiento a partir de sus propias características:

- Adecuación normativa
- Consentimiento para el tratamiento de datos personales
- Mecanismos para cumplir con el principio de responsabilidad
- Medidas de seguridad
- Derechos ARCO
- Comunicaciones de datos personales
- Acciones preventivas
- Órganos responsables
- Medios de impugnación

El límite de esta primera aproximación fue el propio *documento de seguridad* que, en términos de la LGPDPPSO, se conforma de apartados cuya vocación es diagnosticar el estado general en materia de protección de datos personales (análisis de riesgo y de brecha), así como otros apartados que se apoyan en esos dictámenes para detonar las acciones de mediano y largo plazo (plan de trabajo y monitoreo) necesarias para alcanzar y supervisar los propios estándares legales. En suma: la política institucional en materia de datos personales.

2) Inventario de tratamientos de datos personales, *segunda etapa*

La UGTSIJ trabajó con las áreas para la construcción del *inventario de tratamientos de datos personales*, cuya premisa general fue la coordinación interna para localizar todas las bases de datos administrativas en posesión de la SCJN.

El propósito de esta etapa fue identificar cada uno de los procesos en los que las unidades administrativas tratan datos personales. Los elementos que se recogen en el inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa
- Nombre del tratamiento
- Objetivo del tratamiento de datos personales
- Fundamento normativo
- Datos personales que componen la base de datos
- Sensibilidad de los datos personales
- Forma de obtención de los datos personales
- Cargos de las personas que tienen acceso a la base de datos
- Tipo de soporte en el que se almacena la base de datos personales
- Información sobre transferencias de datos personales
- Plazo de conservación

Este ejercicio implicó retroalimentación y acompañamiento permanente para sensibilizar al personal involucrado con el tratamiento de datos personales sobre las obligaciones en la materia, conciliar esquemas que efectivamente implicaban tales tratamientos y definir los formatos para registrarlos.
Para ello, se elaboró un documento denominado "Documento explicativo para el inventario de tratamientos de datos personales de la Suprema Corte de Justicia de la Nación", con la finalidad de exponer los detalles que presenta

el formato del inventario en el que se reportarían los tratamientos de cada área y disipar, en un primer momento, algunas dudas sobre su elaboración **(Anexo 1).**

Una vez que se obtuvo respuesta por parte de las áreas, se les otorgó una clave de identificación a partir del alfabeto para caracterizar cada uno de los tratamientos de los que es responsable (por ejemplo, área: A; tratamientos: A1, A2, A3, así consecutivamente).

De esta forma se integró el documento "Inventario de tratamientos de datos personales", mismo que contiene 80 tratamientos registrados, correspondientes a 21 direcciones y/o unidades generales de la SCJN **(Anexo 2)**.

Cabe precisar que, por sus propias características, es un documento actualizable en caso de que se identifiquen nuevos tratamientos de datos personales o se supriman los que se encuentran identificados.

3) Avisos de privacidad

La implementación del aviso de privacidad en los sujetos obligados tiene como finalidad contar con un instrumento que permita, por un lado, cumplir con el principio de informar a los titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales; y, por otro lado, que los titulares puedan tomar decisiones informadas respecto a dichos tratamientos (artículo 26).

De conformidad con la LGPDPPSO, el aviso de privacidad debe ponerse a disposición de los titulares de manera simplificada al momento de recabar los datos personales y, de manera integral, publicándolo permanentemente en el sitio o medio que se destine para que pueda ser consultado cuando así lo deseen los titulares.

Con la información que se recabó a través del *Inventario de tratamientos de datos personales*, fue posible identificar aquellos en los que, de conformidad con los parámetros normativos, era necesario implementar *avisos de privacidad*.

Para determinar qué tratamientos requerían –o no– *avisos de privacidad*, se partió de la premisa que la LGPDPPSO reconoce una serie de causales de excepción en las que no es necesario recabar el consentimiento (a través del aviso) para que los datos sean tratados con determinado fin.

Por ejemplo, la fracción V del artículo 22 de la LGPDPPSO, expresa que no será necesario recabar el consentimiento cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable. Esta disposición dio la pauta para determinar, en un primer momento, en qué casos era necesario adoptar un aviso de privacidad como medio para la obtención del consentimiento de los titulares de los datos personales, en virtud de que no existe un relación jurídica que pueda justificar el tratamiento.

Por lo tanto, se consideró que todos aquellos tratamientos relacionados con datos personales cuyos titulares no tengan una relación jurídica determinada o determinable con la SCJN y tampoco estén en algún otro supuesto de excepción previsto en la LGPDPPSO, necesitarían un aviso de privacidad. Esto resultó en la adopción de 12 avisos de privacidad, cuyos modelos e información contenidos en cada caso fueron acordados con las propias áreas responsables de su implementación.

Lo anterior quedó reflejado en un documento denominado "Nota informativa sobre el aviso de privacidad" que fue puesto a disposición de las áreas responsables de aquellos tratamientos que requerían de ese instrumento (**Anexo 3**).

Finalmente, los avisos de privacidad simplificados fueron elaborados para que se colocaran en las instalaciones de cada una de las áreas responsables, mientras que los avisos integrales se ubicaron en un repositorio del portal de Internet institucional, en el siguiente enlace: https://www.scjn.gob.mx/transparencia/avisos-privacidad-integral

Los tratamientos que implementaron *avisos de privacidad*, así como las áreas responsables son los siguientes:

Tratamiento	Área responsable
Búsqueda y Préstamos de Expedientes Judiciales	Centro de Documentación y Análisis, Archivos y Compilación de Leyes
Servicio del Sistema Bibliotecario	
Registro de asistentes a eventos del Centro de Estudios Constitucionales	Centro de Estudios Constitucionales
Datos de autores para publicación en el Blog y Foro de la página web del Centro de Estudios Constitucionales	
Inscripción a la Plataforma Electrónica de Acompañamiento y Seguimiento para el Aprendizaje	Dirección General de Casas de la Cultura Jurídica
Expediente Administrativo de los Infantes	Dirección General de Recursos Humanos
Inscripción a Actividades Socioculturales y Recreativas para Jubilados y Pensionados del Poder Judicial de la Federación	
Inscripción a Actividades Socioculturales y Deportivas para el Personal de la Suprema Corte de Justicia de la Nación	
Registro de asistentes a eventos organizados por la DGRI	Dirección General de Relacionales Institucionales
Registro de Entrada y Videograbación por Circuito Cerrado de Televisión	Dirección General de Seguridad
Trámites antes Módulos de Información y Acceso a la Justicia	Unidad General de Transparencia y Sistematización de la Información Judicial

Tratamiento	Área responsable
Registro de Participantes a Cursos y Talleres de la DGEPDDH (virtuales y presenciales)	Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos

4) Guía de protección de datos personales

Como parte de la estrategia de capacitación y sensibilización de los servidores públicos de la SCJN en materia de protección de datos personales, especialmente para aquellos que en sus labores cotidianas realizan tratamientos, la UGTSIJ elaboró y puso a disposición de las áreas que reportaron tratamientos de datos personales, la "Guía de protección de datos personales" que identifica los principios y las bases establecidas en la LGPDPPSO.

Lo anterior con el objetivo de generar un lenguaje común entre las personas involucradas en el tratamiento de datos personales y la UGTSIJ, facilitar las acciones restantes para la construcción del *documento de seguridad* y aproximar conceptos, reglas y parámetros generales e irreductibles para los servidores públicos.

Este documento se distribuyó en formato físico y electrónico, además de publicarse para consumo general en el portal de transparencia, en la siguiente dirección electrónica: https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2019-07/Guia_Proteccion_Datos_Personales_V2.pdf

5) Análisis de riesgos, *tercera etapa*

La UGTISJ emprendió la gestión de un *análisis de riesgo* institucional que, a la postre, identificó los riesgos latentes respecto de cada uno de los tratamientos de datos personales.

Al respecto, es importante contemplar que las medidas de seguridad que adopten las áreas responsables deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello, fue necesario calcular 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.

Para calcular el riesgo latente, se usó la *Metodología de Análisis de Riesgo BAA*, a través de la que es posible calcular los factores antes referidos. Esta metodología se conoce así por las tres variables en las que se enfoca para determinar el nivel de riesgo de los datos personales: i) beneficio para el atacante; ii) accesibilidad para el atacante; y iii) anonimidad del atacante.[2]

Para contar con la información relacionada al riesgo, la UGTSIJ realizó acciones diversas, algunas de las cuales se describen a continuación:

En primer lugar, con el propósito de proveer un marco general y acercar a las áreas a las particularidades de este tema, confeccionó un documento denominado "Medidas de seguridad y análisis de riesgo de datos personales" **(Anexo 4)**.

Este insumo procuró sensibilizar a las personas involucradas con el tratamiento de los datos personales y los parámetros legales que promueven el uso adecuado de los mismos, cuya finalidad es garantizar la confidencialidad y los derechos de protección de los datos personales que son utilizados en el trabajo cotidiano de las propias áreas.

[2] "Metodología de Análisis de Riesgo BAA", Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, junio 2015. http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

El contenido incluyó los conceptos básicos en la materia, la definición y tipos de medidas de seguridad, la categorización de los datos personales y la metodología para calcular el riesgo latente.

En segundo lugar y con la finalidad de analizar datos objetivos, actuales y fidedignos para la elaboración del *análisis de riesgo*, se diseñó y aplicó la "Encuesta sobre análisis de riesgos y medidas de seguridad" **(Anexo 5).**

Esta encuesta retomó cada uno de los tratamientos que habían sido previamente reportados y registrados en el inventario de tratamientos de datos personales por cada área. Se aplicaron 80 encuestas entre las 21 áreas administrativas que reportaron tratamientos de datos personales.

En tercer lugar y priorizando esquemas de intercambio, solución de dudas y homologación de criterios para solventar la encuesta, se organizó un *Taller de acompañamiento* con los enlaces designados por cada instancia administrativa ante la UGTSIJ.

En el taller se desarrollaron temas como la definición de un documento de seguridad, el propósito del inventario de tratamientos de datos personales, la función de un aviso de privacidad, la metodología del análisis de riesgos (BAA), la función del análisis de brecha y los mecanismos de seguimiento. Contó con la asistencia de 16 enlaces y/o personal encargado de tratamientos, correspondientes a 15 áreas administrativas de la SCJN.

Derivado de la celebración del taller, se realizaron reuniones específicas con áreas determinadas, entre las que destacan la Secretaría General de la Presidencia; la Dirección General de Presupuesto y Contabilidad; la Dirección General de Relaciones Institucionales; la Dirección General de Seguridad; y, la Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos.

Finalmente, se calculó el *riesgo latente por tratamiento*, lo que permitiría definir el esquema de medidas de seguridad para cada uno de acuerdo al nivel de riesgo.

Este cálculo acudió a los parámetros delineados en el documento *Medidas de seguridad y análisis de riesgo de datos personales* y consideró 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.

En ese sentido, se advirtió que a partir del tipo de dato es posible reconocer el factor de riesgo inherente, al cual es necesario sumarle el volumen de titulares contenidos en la base de datos, lo que da como resultado el *nivel de riesgo por tipo de dato*. A su vez, el nivel de riesgo por tipo de dato servirá para determinar los controles que se deben considerar para su protección.

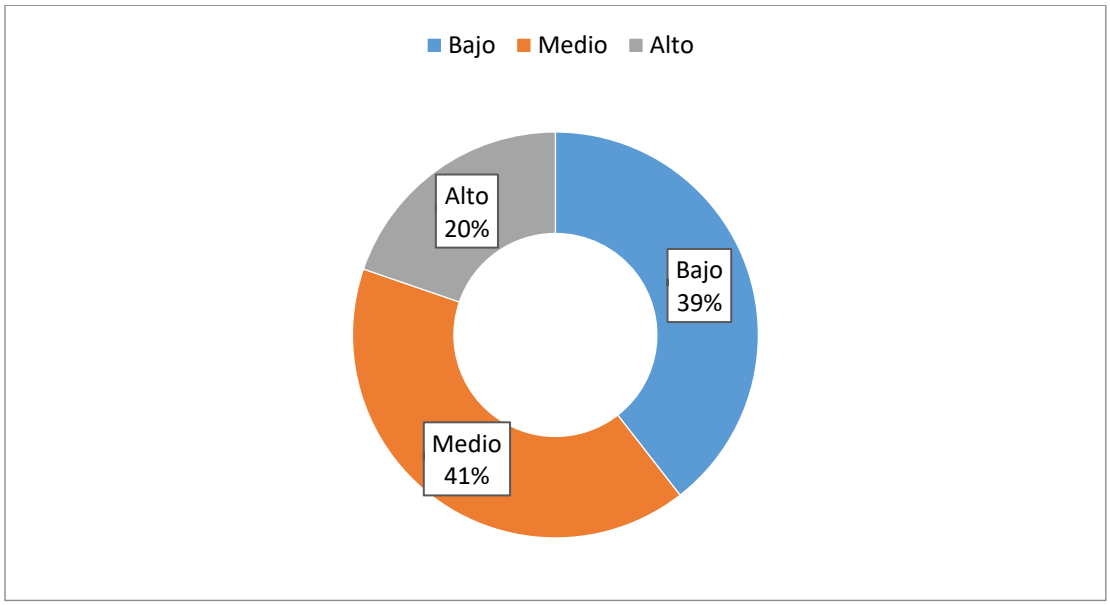
Por otra parte, el *riesgo por tipo de acceso* se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo. Para este parámetro entre mayor sea la accesibilidad, mayor riesgo existe para la información.

Finalmente, el *riesgo por tipo de entorno* representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad. En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

En suma, la combinación de los tres factores analizados permitió a la UGTSIJ definir el nivel de *riesgo latente por tratamiento*, lo cual contribuirá a identificar el nivel de medidas de seguridad que deban implementarse en cada caso **(Anexo 6).**

La **GRÁFICA 1** ilustra la cantidad de tratamientos que se ubican en un nivel de riesgo alto, medio o bajo, según sea su caso:

GRÁFICA 1. NÚMERO DE TRATAMIENTOS CLASIFICADOS POR NIVEL DE RIESGO



Una vez que se calculó el *nivel de riesgo latente* por cada tratamiento de datos personales, fue posible diseñar estrategias para identificar los modelos de medidas de seguridad que debían aplicarse a cada uno de ellos.

6) Análisis de brecha, *cuarta etapa*

La UGTSIJ elaboró un *análisis de brecha* consistente en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, cuya información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar. Lo anterior con el objetivo de atenderlas de manera escalonada y en coordinación con cada una de las áreas.

Como medida previa a este análisis se confeccionó un "Catálogo de medidas de seguridad para los tratamientos de datos personales" **(Anexo 7).**

El referido catálogo se construyó a partir de los parámetros normativos y buenas prácticas que se desprenden de la propia LGPDPPSO, las políticas institucionales de seguridad de la SCJN y la asesoría de la Dirección General de Tecnologías de la Información.

En este documento se describen las medidas de seguridad administrativas, físicas y técnicas –complementarias a las políticas de seguridad generales de la SCJN– para los tratamientos de datos personales en la institución. Además, se incluyen recomendaciones generales de medidas de seguridad para cada tratamiento, tomando como referencia el nivel de riesgo latente que fue reportado.

Posteriormente y teniendo como referencia el citado catálogo, se elaboró la "Encuesta sobre análisis de brecha" **(Anexo 8),** con la finalidad de identificar las medidas de seguridad recomendadas para cada uno de los tratamientos de las áreas responsables, y que éstas informaran sobre aquellas ya implementadas y las que aún están pendientes.

Lo principales resultados del *análisis de brecha* **(Anexo 9),** arrojaron lo siguiente:

La GRÁFICA 2 muestra el porcentaje de tratamientos en distintos niveles de cumplimiento con las medidas de seguridad.

GRÁFICA 2. PORCENTAJE DE TRATAMIENTOS POR NIVEL DE CUMPLIMIENTO CON MEDIDAS DE SEGURIDAD

7) Programa de capacitación

El Programa de Capacitación en materia de transparencia, acceso a la información y protección de datos personales 2019, aprobado por el Comité de Transparencia, y dirigido a los enlaces de transparencia, responsables de Módulos de Información y Acceso a la Justicia (MIAJ) e integrantes de la UGTSIJ, incluye cursos virtuales relacionados con la materia, a saber:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Clasificación y desclasificación de la Información
- Metodología, diseño y formulación sistemas clasificación y ordenación archivística

Además, el Programa de Capacitación incluye un curso presencial en materia de protección de datos personales impartido por el Instituto Tecnológico Autónomo de México (ITAM) a las y los integrantes de la UGTSIJ.

III. Asignaturas pendientes

El trabajo realizado hasta el momento revela una serie de aspectos para contemplar en el horizonte inmediato. Algunos tienen que ver con la necesidad de vislumbrar mecanismos de factibilidad, competencia, implementación, monitoreo y revisión de las medidas de seguridad recomendadas en el marco de las atribuciones del propio Comité de Transparencia y como elemento esencial del *documento de seguridad*; mientras que otras resultan de las particularidades, dudas y definiciones de áreas específicas de la SCJN.

Para formular lo anterior, en primer lugar, es importante generar esquemas de trabajo interdependientes con aquellas áreas que juegan un papel trascendental en la protección de los datos personales a nivel institucional. En este caso se encuentran áreas como la Dirección General de Seguridad, la Dirección General de Tecnologías de la Información y el Centro de Documentación y Análisis, Archivos y Compilación de Leyes.

Por otro lado, es relevante desarrollar un esquema de acompañamiento con cada una de las áreas con la finalidad de acortar la brecha hacia el cumplimiento total de las medidas de seguridad recomendadas, tomando en cuenta los factores normativos y obstáculos prácticos a los que las áreas se enfrentan cotidianamente.

Algunos pendientes a resolver en una segunda etapa es la inclusión, en este esquema, de los tratamientos de datos personales realizados en las Casas de la Cultura Jurídica de este Alto Tribunal, debiéndose impulsar la coordinación

con la dirección general respectiva para nivelar los propios tratamientos y los esquemas de protección en dichas instancias.

Además, resulta indispensable valorar los tratamientos de datos personales registrados, para evaluar si cumplen con los principios de licitud, finalidad, lealtad, calidad, proporcionalidad, consentimiento, información y responsabilidad, que mandata la LGPDPPSO.

Finalmente, algunas áreas han expresado su inquietud para adoptar leyendas o cláusulas de protección de datos personales en los contratos celebrados con terceros para el desarrollo de sus actividades o para la implementación de buenas prácticas que refuercen la confidencialidad de los datos personales sensibles como los que obran en expedientes médicos.

IV. Conclusiones

Este documento ofrece una radiografía institucional en materia de protección de los datos personales en su faceta administrativa, refleja sus fortalezas, pendientes y áreas de oportunidad, y constituye un insumo actual para la toma de decisiones por parte de las instancias competentes en ese renglón.

A partir de las acciones relatadas se modeló un estado de cosas que revela necesidades particulares de la SCJN para el diseño de planes de trabajo, implementación, factibilidad, mecanismos de monitoreo y revisión de medidas de seguridad, así como programas de capacitación generales, elementos que también integran el *documento de seguridad* y son imprescindibles para que el Comité de Transparencia disponga lo conducente en torno a estas medidas institucionales.

Es importante contemplar que el *documento de seguridad* representa, además de una obligación legal, un instrumento vital para la coordinación de los trabajos de todas las áreas de la SCJN encaminados al fortalecimiento y mejora en el tratamiento e implementación de medidas de seguridad de los datos personales bajo su resguardo.

V. Anexos

ANEXO 1. Documento explicativo para Inventario de tratamientos de datos personales

I. PRESENTACIÓN

En semanas pasadas, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través del Programa Modelo de Protección de Datos Personales, puso a disposición herramientas modelo que permiten desarrollar y materializar algunas obligaciones que enmarca la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO).

Entre estas herramientas modelo, se encuentra el formato para realizar el Inventario de Tratamientos en los sujetos obligados, lo que permitirá, como primer esfuerzo institucional, contar con un censo amplio que permita brindar un panorama general de las bases de datos que manejan las áreas de este Alto Tribunal.

Contar con un Inventario de Tratamientos de Datos Personales de la Suprema Corte de Justicia de la Nación, permitirá detonar los siguientes esfuerzos que brinden la posibilidad de contar con los elementos institucionales necesarios y estar acorde a los nuevos estándares en la materia, conforme a los plazos transitorios.

Para ello, la herramienta ha sido adecuada para que las áreas de este Alto Tribunal puedan informar con puntualidad los diversos tratamientos de datos personales que llevan en sus actividades y que esta Unidad General tenga la posibilidad de tener un análisis puntual y detallado de cada una de las áreas.

Una vez que se haya realizado este diagnóstico inicial, estaremos preparados para cumplir de mejor manera con las obligaciones previstas en la LGPDPPSO.

A continuación se explican algunos detalles que presenta el formato del Inventario para despejar, *a priori*, algunas dudas en su elaboración, puntualizando que la propia Unidad General brindará apoyo si así lo consideran necesario las propias áreas.

II. EXPLICACIÓN DEL FORMATO.

1. ¿Qué es el Inventario de Tratamientos y a quién está dirigido?

Es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario de los tratamientos de datos personales que se realizan en la Suprema Corte de Justicia de la Nación.

Por "inventario de tratamientos" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas, realizado con orden y precisión.

El inventario de tratamientos incluirá el inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III y 35, fracción I, e identificará los siguientes elementos relevantes.

2. ¿Qué tratamientos de datos personales realiza la unidad administrativa?

Identificar cada uno de los procesos en los que la unidad administrativa trata datos personales. Por tanto, el formato corresponde a cada uno de los tratamientos que realiza el área en razón de que se deben enlistar los tipos de tratamientos y cada uno de los datos personales que son usados para ello. Por ejemplo, en caso de que el área realice dos tratamientos, ésta deberá llenar dos formatos.

3. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?

Identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta; sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

4. ¿Qué es un tratamiento de datos personales?

De conformidad con el artículo 3, fracción XXXIII de la LGPDPPSO, un tratamiento es 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, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario identificar lo siguiente, de acuerdo con el ciclo de vida de los datos personales.

a. ¿Cómo se obtienen los datos personales?

Los numerales (1) al (4) dentro del formato se encargan de recabar de especificar de dónde se obtienen los datos personales.

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
    - Vía telefónica
    - Por correo electrónico
    - Por Internet o sistema informático
    - Por escrito presentado directamente en [*nombre de la institución*]
    - Por escrito enviado por mensajería

- Mediante una transferencia
    - Quién transfiere los datos personales y para qué fines
    - Medios por los que se realiza la transferencia

- De una fuente de acceso público

b. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

Los numerales (5) y (6) se encargan de enlistar los diversos tipos de datos personales que se usan en un tratamiento de datos personales. En este caso, es indispensable mencionar cada dato personal por fila e identificar si se trata de un dato personal sensible o no en la columna correspondiente.

De conformidad con el artículo 3, fracción X de la LGPDPPSO, son 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.

c. ¿Dónde se almacenan los datos personales?

Los numerales del (7) al (11) se encargan de ubicar el formato en que se almacenan los datos personales y también los datos de ubicación de dichos archivos tomando los siguientes elementos:

- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos
- Sección, serie y subserie de archivos

En caso de contar con otro tipo de clasificación o identificación de la sección a la que corresponde la base de datos especificarlo, o en caso contrario especificar que no se cuenta con tal.

d. ¿Para qué finalidades se utilizan los datos personales?

Los numerales (12) a (15) se encargan de registrar las finalidades del tratamiento y si éstas requieren consentimiento del titular.

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser "recursos de revisión" y las finalidades "emitir los acuerdos y notificaciones correspondientes, y entrar en contacto con el recurrente con fines de orientación".

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos (fracciones) del artículo 22 se actualizan.

e. ¿Quién tiene acceso a la base de datos o archivos y a quién se comunican los datos personales al interior?

Los numerales (16) y (17) se encargan de registrar estos datos. Se deberá identificar el catálogo de servidores públicos al interior del área que tienen acceso a los datos personales y para qué fin.

f. ¿Intervienen encargados en el tratamiento de los datos personales?

Los numerales (18) y (19) especifican si las bases de datos son manejados por un encargado a nombre del área o la propia institución, y se debe identificar el instrumento por el que dicha relación jurídica se sustenta.

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente. Un encargado es la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable. Por ejemplo, una empresa que se encargue de manejar una base de datos para brindar un software de seguridad a nombre del área pero que no implique la transferencia de datos personales.

g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

Los numerales (20) al (26) se encargan de la actividad de la transferencia de bases de datos fuera de la institución.

Una transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o encargado.

Hay que identificar las autoridades o terceros externos a la institución a quienes se comunican los datos personales y los fines de las transferencias.

Asimismo, es necesario señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 se actualizan.

h. ¿Se difunden los datos personales?

Los numerales (28) y (29) se encargan de registrar si las bases de datos son difundidas al público por cualquier motivo. Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

i. ¿Cuál es el plazo de conservación de los datos personales?

El numeral (30) se encarga de este dato. Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

ANEXO 2. Inventario de tratamientos de datos personales

A. Dirección General de Recursos Humanos.

A.1 Evaluación Psicométrica

1. **Objetivo:** los datos personales son recabados para realizar la aplicación de evaluación psicométrica para cumplir con la normativa establecida.
2. **Fundamento:** Artículo 22, fracción I del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Año de nacimiento o edad.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Nacionalidad.
   - **Discapacidad – Sensible.**
   - Nivel educativo.
   - Curriculum vitae.
   - Firma.
   - Datos académicos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Profesional operativo.
   - Técnico operativo.
   - Subdirector de área.
6. **Tipo de soporte**
   - Archivero de la unidad (serie: MX-SCJN-RH-03).
   - Equipo de cómputo.
7. **Transferencias**: no.

8. **Plazo de conservación**: 25 años.

A2. Servicio Social

1. **Objetivo**: dar cumplimiento a los programas de servicio social autorizados en este Alto Tribunal.
2. **Fundamento:** Artículo 22, fracción II del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Año de nacimiento o edad.
   - Nivel educativo.
   - Curriculum vitae.
   - Firma.
   - Datos académicos.
4. **Forma de obtención**:
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Jefe(a) de departamento.
6. **Tipo de soporte:**
   - Archivero de la unidad administrativa (serie: MX-SCJN-RH-07).
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

A3. Expedientes de Personal

1. **Objetivo:** control y resguardo de datos y documentos personales de los servidores públicos.

2. **Fundamento:** Artículo 22, fracción V del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Persona fallecida.
   - Datos personales contenidos en la descripción del trámite o realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Curriculum vitae.
   - **Datos de salud – Sensible.**
   - Descuentos personales.
   - **Datos personales de beneficiarios – Sensible tratándose de menores de edad.**
   - Firma.
   - Datos personales contenidos en documento para acreditar personalidad del representante.
   - Datos académicos.
   - Datos laborales.
   - **Información migratoria – Sensible.**
   - CURP
   - RFC
   - Fotografía.
   - **Evaluación Psicométrica – Sensible.**
   - Acta de nacimiento.
   - Cuenta bancaria.
   - **Dictamen de invalidez – Sensible.**
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.

- Correo electrónico.
- Oficio presentado por los titulares de órganos y áreas.

5. **Cargos que tienen acceso a la base de datos:**
   - Director de ingreso y control de personal.
   - Subdirector de expedientes.
6. **Tipo de soporte:**
   - Archivero de la unidad administrativa (sección: MX-SCJN-RH-04).
   - Equipo de cómputo.
   - Servidor de la institución.
   - Archivo de concentración.
7. **Transferencias:** No.
8. **Plazo de conservación:** Sin plazo.

A4. Fondo de Ahorro Capitalizable (FONAC)

1. **Objetivo**: Los servidores públicos se dan de alta en el sistema SAP para llevar el control de las aportaciones quincenales de la liquidación anual (12 y 24 QNAS).
2. **Fundamento**: Artículo 22, fracciones I, II, IV y XVI del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Persona fallecida.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.
   - Año de nacimiento o edad.
   - **Beneficiarios – Sensible tratándose de menores de edad.**
   - Firma.
   - CURP.
   - RFC.
   - **Dictamen de Invalidez – Sensible.**
4. **Forma de obtención:**
   - Escrito.
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**

- Director(a) de nómina.
- Subdirector(a) de remuneraciones.
- Jefe(a) de departamento.
- Profesional operativo.

6. **Tipo de soporte:**
   - Archiveros de la unidad administrativa (sección: MX-SCJN-RH-15).
   - Servidor de la institución.
7. **Transferencias:** las transferencias se realizan con la finalidad de la liquidación anual del FONAC.
   - BANORTE.
8. **Plazo de conservación:** permanente.

A.5 Procesamiento de información para obtener cifras que se envían a terceros institucionales públicos y privados (juzgados familiares, ISSSTE, FOVISSSTE, bancos y beneficiarios particulares por disposición judicial)

Objetivo: dirigir las actividades que se derivan de los descuentos por concepto de Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, Fondo de la Vivienda del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, Juzgados Familiares, Juzgados Civiles, Colegio de Secretarios, Colegio de Estudiantes y Deportivo Hacienda, entre otros.

1. **Fundamento**: Artículo 22, fracciones I, II, IV, V, XII y XVI del Reglamento Orgánico en Materia de Administración.
2. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Persona fallecida.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Año de nacimiento o edad.
   - **Beneficiarios – Sensible tratándose de menores de edad.**
   - Firma.
   - CURP.
   - RFC.
   - **Dictamen de Invalidez – Sensible.**
   - Recibo de Nómina.
   - Datos bancarios.

3. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.
   - Del FOVISSSTE se obtiene la información del sistema SICIOD en internet. Del ISSSTE, la información llega a través de un CD y por correo electrónico.
4. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de nómina.
   - Subdirector(a) de remuneraciones.
   - Jefe(a) de departamento de procesamiento de nómina.
   - Jefe(a) de departamento de control y análisis.
   - Profesionales operativos.
5. **Tipo de soporte:**
   - Servidor de la institución.
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
6. **Transferencias:** para la actualización de los descuentos realizados y su afectación en sus bases de datos, para la aplicación de descuentos y deducciones, para el interés particular del o de los beneficiarios.
   - ISSSTE y FOVISSSTE
   - CJF y TEPJF
   - Banorte, Qualitas, Metlife, Colegio de Estudiantes, Colegio de Secretarios, Domani, HSBC, entre otros.
   - Juzgados familiares.
   - Beneficiarios de pensiones alimenticias.
7. **Plazo de conservación:** permanente.

A.6 Sistema de Ahorro para el Retiro (SAR).

1. **Objetivo**: Calcular los importes de las aportaciones al SAR, ISSSTE, FOVISSSTE y Ahorro Solidario de los trabajadores de la SCJN para envío a la empresa operadora que realiza la dispersión de dichas aportaciones a las diversas Afores.
2. **Fundamento**: Artículo 22, fracciones I y XII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.

- Persona fallecida.
- Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
- Domicilio.
- Sexo.
- Año de nacimiento o edad.
- CURP.
- RFC.

4. **Forma de obtención:**
   - Servidor de la institución.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de nómina.
   - Subdirector(a) de remuneraciones.
   - Jefe(a) de departamento.
   - Profesionales operativos.
6. **Tipo de soporte:**
   - Servidor de la institución (sección: MX-SCJN-RH-17.4).
7. **Transferencias:** para efectuar la dispersión de las aportaciones al SAR, ISSSTE, FOVISSSTE y Ahorro Solidario a la Afore de cada trabajador.
   - SIRI PROCESAR
8. **Plazo de conservación**: permanente.

A.7 Elaboración de Contratos por Honorarios Asimilados a Salarios

1. **Objetivo:** Suscribir los contratos de prestación de servicios profesionales subordinados asimilables a salarios autorizados.
2. **Fundamento:** Artículo 22, fracción XI del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Domicilio.
   - Sexo.
   - Año de nacimiento o edad.
   - Nivel educativo.
   - Firma.
   - Datos académicos.
   - Títulos o constancias académicas.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de relaciones laborales.
   - Subdirector(a) de área.
   - Profesionales operativos.
6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
7. **Transferencias:** No.
8. **Plazo de conservación**: 12 años.

A.8 Becas - SCJN

1. **Objetivo:** Gestionar el apoyo económico otorgado al trabajador.
2. **Fundamento**: Artículo 22, fracción XX del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Sexo.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Nivel educativo.
   - Firma.
   - Títulos profesionales.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Datos bancarios.
4. **Forma de obtención:**
   - A través del formato signado por el titular del órgano o área requirente.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Jefe(a) de departamento.
   - Profesionales operativos.
   - Técnicos operativos.

6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa (sección: MX-SCJN-RH-20-1).
   - Archivo de concentración.
   - USB, disco duro externo.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años.

A.9 Capacitación

1. **Objetivo:** Gestionar el pago de los servicios de capacitación.
2. **Fundamento:** Artículo 22, fracción XX del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Sexo.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Curriculum vitae.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Datos bancarios.
4. **Forma de obtención:**
   - A través del formato signado por el titular del órgano o área requirente.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Técnicos operativos.
6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
   - USB.
   - Disco duro externo.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años.

A.10 Prácticas judiciales

1. **Objetivo:** Gestionar el apoyo económico del estudiante postulado.
2. **Fundamento:** Artículo 22, fracción II del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Sexo.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Curriculum vitae.
   - Año de nacimiento o edad.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Datos bancarios.
   - Nivel educativo.
   - Firma.
   - Títulos o constancias profesionales.
   - Datos académicos.
4. **Forma de obtención:**
   - A través del formato signado por el titular del órgano o área requirente.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Profesionales operativos.
6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
   - USB, disco duro externo.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años.

A.11 Trámite para el Apoyo y Ayuda de Anteojos

1. **Objetivo**: Dar trámite a la solicitud de apoyo y ayuda de anteojos.
2. **Fundamento:** Artículo 22, fraccione XXXII y XXXIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.

- Teléfono fijo o celular.
- Año de nacimiento o edad.
- **Datos de salud – Sensible.**
- Firma.
- **Beneficiarios – Sensible tratándose en caso de menores.**
- Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Programas Sociales.
   - Jefe(a) de departamento de seguimiento y control de programas.
   - Profesionales operativos.
   - Técnicos operativos.
6. **Tipo de soporte:**
   - Equipo de cómputo.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años.

A.12 Inscripción a Actividades Socioculturales y Deportivas para el personal de la SCJN

1. **Objetivo:** Inscribir a las personas interesadas en participar en las Actividades Socioculturales y Deportivas para el personal de la SCJN.
2. **Fundamento:** Artículo 22, fracción XX del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Teléfono fijo o celular.
   - Sexo.
   - **Datos de salud – Sensible.**
   - Correo electrónico.
   - Nombre de familiar para avisar en caso de emergencia.
   - Teléfono de familiar para avisar en caso de emergencia.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**

- Director(a) de Programas Sociales.
- Subdirector(a) de área.
- Jefe(a) de departamento de Actividades Culturales y Deportivas.
- Profesionales operativos.
- Técnicos operativos.

6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años

A.13 Inscripción a Actividades Socioculturales y Recreativas para Jubilados y Pensionados del PJF

1. **Objetivo:** Inscribir a las personas interesadas en participar en las Actividades Socioculturales y Recreativas para Jubilados y Pensionados del PJF.
2. **Fundamento:** Artículo 22, fracción XX del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Teléfono fijo o celular.
   - Sexo.
   - **Datos de salud – Sensible.**
   - Correo electrónico.
   - Año de nacimiento o edad.
   - Firma.
   - **Características físicas – Sensible.**
   - Nombre de familiar para avisar en caso de emergencia.
   - Teléfono de familiar para avisar en caso de emergencia.
   - Información de participación en asociaciones.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Programas Sociales.
   - Subdirector(a) de área.
   - Profesionales operativos.

- Técnicos operativos.

6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa.
7. **Transferencias:** No.
8. **Plazo de conservación:** 6 años.

A.14 Expediente Administrativo de los Infantes

1. **Objetivo:** Los datos personales son recabados por parte del personal de la DGPSI, con la finalidad de ofrecer un servicio educativo y de desarrollo integral de los hijos e hijas de las personas trabajadoras de la Suprema Corte, en tanto se encuentran en su horario laboral.
2. **Fundamento:** Artículo 22, fracciones XXI y XXII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre(s) y apellido(s) de persona física, madre, padre o tutor.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - **Datos personales contenidos en documento para acreditar parentesco (acta de nacimiento) – Sensible.**
   - **Datos personales contenidos en la solicitud de inscripción – Sensible.**
   - Domicilio.
   - Correo electrónico.
   - Número de teléfono.
   - **Datos socioeconómicos – Sensible.**
   - Firma.
   - **Datos sensibles del infante:**
     - **Nombre.**
     - **Información médica.**
     - **Intervenciones realizadas para la atención en conducta, lenguaje, emocional y cognitiva.**
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Coordinador(a) administrativa.
   - Subdirector(a) pedagógica.

- Subdirector(a) de cursos y talleres.
- Subdirector(a) técnica.
- Profesionales operativos.

6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa (sección: MX-SCJN-RH-22).
7. **Transferencias**: la finalidad de la transferencia es llevar el registro escolar de los infantes ante la autoridad educativa correspondiente.
   - Secretaría de Educación Pública
8. **Plazo de conservación:** 12 años.

A.15 Expediente Administrativo de Apoyo Económico

1. ***Objetivo***:
2. **Fundamento:** Artículo 22 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos de representante.
   - Nombre y apellidos de menor.
   - Datos contenidos en la identificación oficial presentada por la persona física.
   - Datos contenidos en documento para acreditar parentesco (acta de nacimiento).
   - Datos contenidos en la solicitud de apoyo.
   - Firma.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Coordinador(a) administrativa.
6. **Tipo de soporte:**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa (sección: MX-SCJN-RH-22).
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

A.16 Movimientos Afiliatorios ante el ISSSTE

1. **Objetivo:** Control y seguimiento de movimientos enviados al ISSSTE.

2. **Fundamento:** Ley del Instituto de Seguridad y Servicio Social de los Trabajadores del Estado.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Año de nacimiento o edad.
   - RFC.
   - CURP.
4. **Forma de obtención:**
   - Sistema Integral de Administración.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Administración de Personal.
   - Subdirector(a) de Movimientos Jurisdiccionales.
   - Jefe(a) de Departamento de Afiliación al ISSSTE.
6. **Tipo de soporte:**
   - Equipo de cómputo (ZPC00_M32_PBS_UACT).
   - Servidor de la institución.
7. **Transferencias:** para dar cumplimiento al ordenamiento de la Ley del ISSSTE en lo relativo a movimientos afiliatorios.
   - ISSSTE.
8. **Plazo de conservación:** Indefinido.

A.17 Registro de datos personales en el Seguro de Separación Individualizado

1. **Objetivo:** Inscripción al Seguro de Separación Individualizado y designación de beneficiarios.
2. **Fundamento:** Artículo 22 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Sexo.
   - Año de nacimiento o edad.
   - Datos laborales.
   - Beneficiarios.
   - **Menor de edad – Sensible.**
   - Firma.
   - RFC.
   - Parentesco de los beneficiarios.

- **Fecha de nacimiento de los beneficiarios asegurados – Sensible tratándose de menores de edad.**
- Estado Civil.
- CURP.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) General de Seguros.
   - Subdirector(a) de Seguros, Fondos y Daños.
   - Profesional operativo.
6. **Tipo de soporte:**
   - Equipo de cómputo.
7. **Transferencias:** Administrar y dar servicio a los asegurados de las pólizas.
   - Metlife México, S.A.
8. **Plazo de conservación:** Conforme al contrato vigente.

A.18 Registro de datos personales en el Seguro de Vida e Invalidez Total y Permanente

1. **Objetivo:** Inscripción al Seguro de Vida e Incapacidad Total y Permanente, así como designación de beneficiarios.
2. **Fundamento:** Artículo 22 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Sexo.
   - Año de nacimiento o edad.
   - Datos laborales.
   - Beneficiarios.
   - **Menor de edad – Sensible.**
   - Firma.
   - RFC.
   - Parentesco de los beneficiarios.
   - Correo electrónico.
   - CURP.
4. **Forma de obtención:**

- De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
- Internet o sistema informático.

5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) General de Seguros.
   - Subdirector(a) de Personal.
   - Profesional operativo.
6. **Tipo de soporte:**
   - Equipo de cómputo.
7. **Transferencias:** Administrar y dar servicio a los asegurados de las pólizas.
   - Seguros Banorte S.A. de C.V.
   - Grupo Financiero Banorte.
8. **Plazo de conservación:** Conforme al contrato vigente.

A.19 Registro de datos personales en el Fondo de Reserva Individualizado

1. **Objetivo**: Inscripción al Fondo de Reserva Individualizado y designación de beneficiarios.
2. **Fundamento**: Artículo 22 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Menor de edad.
   - Firma.
   - RFC.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) General de Seguros.
   - Subdirector(a) de Personal.
   - Profesional operativo.
6. **Tipo de soporte:**
   - Equipo de cómputo.
7. **Transferencias:** Administrar y dar servicio a los servidores registrados en el fondo.
   - Principal Fondos de Inversión S.A. de C.V.
8. **Plazo de conservación:** Conforme al contrato vigente.

A.20 Registro de datos personales en el Seguro de Gastos Médicos Mayores

1. **Objetivo:** Inscripción al Seguro de Gastos Médicos Mayores, así como la inclusión de sus beneficiarios.
2. **Fundamento:** Artículo 22 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Sexo.
   - Año de nacimiento o edad.
   - Beneficiarios.
   - **Menor de edad – Sensible.**
   - Firma.
   - Correo electrónico.
   - RFC.
   - Edad de los beneficiarios asegurados.
   - Parentesco de los beneficiarios asegurados.
   - Sexo de los beneficiarios asegurados.
   - Estado civil.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) General de Seguros.
   - Subdirector(a) de Personal.
   - Profesional operativo.
6. **Tipo de soporte:**
   - Equipo de cómputo.
7. **Transferencias:** Administrar y dar servicio a los servidores registrados en el fondo.
   - Principal Fondos de Inversión S.A. de C.V.
8. **Plazo de conservación**: Conforme al contrato vigente.

B. Dirección General de la Coordinación de Compilación y Sistematización de Tesis

B1. Suscripción a la Gaceta del Semanario Judicial de la Federación y venta de publicaciones

1. **Objetivo:** los datos personales son recabados para realizar la suscripción a la Gaceta y para emitir facturas.
2. **Fundamento:** Acuerdo General de Administración II/2008 del Comité de Publicaciones y Promoción Educativa de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Jefe(a) de departamento.
   - Profesional operativo.
   - Técnico operativo.
   - Secretario(a).
6. **Tipo de soporte**
   - Archivero de la unidad (TP-04.5).
   - Equipo de cómputo.
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

B2. Emisión de constancias por asistencia a curso de capacitación

1. **Objetivo**: Emitir la constancias de participación en el curso.
2. **Fundamento:** Artículo 149, fracción VIII del Reglamento Interior de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.

4. **Forma de obtención**:
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Dictaminador(a) II.
6. **Tipo de soporte:**
   - Archivero de la unidad administrativa (TP-07.1).
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE RECURSOS MATERIALES.

Dirección General de Recursos Materiales

C1. Proveedores de bienes y servicios

1. **Objetivo:** los datos personales son recabados para girar invitaciones para participar en eventos concursales y acreditar domicilio legal para enviar notificaciones.
2. **Fundamento:** *no reportado*.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Firma.
   - Datos bancarios.
   - RFC.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Adquisición de Bienes Informáticos, Comunicaciones y Materiales Bibliohemerográficos.
   - Subdirector(a) de Adquisición de Bienes Informáticos.
   - Jefe(a) de departamento.
   - Profesional operativo.
   - Técnico operativo.
   - Secretario(a).
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: *no reportado*.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE RELACIONES INSTITUCIONALES.

Dirección General de Relaciones Institucionales

D1. Registro de asistentes a eventos organizados por la DGRI

1. **Objetivo:** los datos personales son recabados para registrar a las personas interesadas en asistir a un evento; elaborar listas de asistencia; elaborar constancias de asistencias; generar estadísticas sobre los asistentes al evento; enviar invitaciones a futuros eventos.
2. **Fundamento:** Artículo 18, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Firma.
   - Institución a la que pertenece.
   - Cargo.
4. **Forma de obtención:**
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Jefe(a) de departamento.
   - Profesional operativo.
   - Técnico operativo.
   - Asesor(a).
6. **Tipo de soporte**
   - Archivero de la unidad (serie: MX-SCJN-RI-08).
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

D2. Realizar invitaciones a eventos y envío de libros

1. **Objetivo:** los datos personales son recabados para realizar invitaciones para participar como ponente en eventos; enviar los libros editados con motivo de los eventos organizados; elaborar el programa de los eventos; elaborar constancias de participación.
2. **Fundamento:** Artículo 18, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Domicilio.
   - Teléfono fijo o celular.
   - Institución a la que pertenece.
   - Cargo.
4. **Forma de obtención:**
   - Vía telefónica.
   - Correo electrónico.
   - Fuentes de acceso público.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Profesional operativo.
   - Técnico operativo.
   - Dictaminador(a) II.
6. **Tipo de soporte**
   - Equipo de cómputo (serie: MX-SCJN-RI-05).
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

D3. Registro de estancias de estudio y visitas oficiales al extranjero

1. **Objetivo:** Contar con la relación de servidores públicos que participan en las estancias o visitas en el extranjero; elaborar listas de asistencia; elaborar las constancias de

asistencia; elaborar informes y reportes sobre las actividades realizadas; apoyar en la logística de las actividades y tramitar los accesos a los sitios a visitar en el extranjero.

2. **Fundamento:** Artículo 18, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Domicilio.
   - Teléfono fijo o celular.
   - **Datos de salud – Sensible.**
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Curriculum vitae.
   - Copia del pasaporte.
   - Datos sobre viaje (duración, hospedaje vuelos).
4. **Forma de obtención:**
   - Vía telefónica.
   - Correo electrónico.
   - Fuentes de acceso público.
5. **Cargos que tienen acceso a la base de datos:**
   - Dictaminador(a).
   - Asesor(a).
   - Coordinador(a) Administrativo(a).
6. **Tipo de soporte**
   - Equipo de cómputo (serie: MX-SCJN-RI-05).
7. **Transferencias**: Tramitar los accesos a los sitios a visitar en el extranjero:
   - Organismos jurisdiccionales internacionales y regionales.
   - Poderes judiciales extranjeros.
   - Universidades extranjeras.
   - Organizaciones internacionales.
8. **Plazo de conservación**: 6 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL.

E. Dirección General de Comunicación Social

E1. Boletín Electrónico de la Suprema Corte

1. **Objetivo:** Enviar el boletín vía correo electrónico y contar con datos para fines estadísticos.
2. **Fundamento:** Artículo 14, fracción VIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Año de nacimiento o edad.
   - Entidad Federativa.
4. **Forma de obtención:**
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Sistema informático institucional.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E2. SIA

1. **Objetivo:** los datos personales son recabados para registro de ventas por cliente.
2. **Fundamento:** Artículo 14, fracción VIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - RFC
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.

- Profesional operativo.

6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E3. Sistema Electrónico de Registro de Eventos (ya no se usa)

1. **Objetivo:** Fines estadísticos e invitación a nuevos eventos.
2. **Fundamento:** Artículo 14, fracción XIV del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Año de nacimiento o edad.
   - Sexo.
   - Domicilio.
   - Teléfono fijo o celular.
   - Correo electrónico.
   - Datos académicos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) General.
   - Profesional operativo.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E4. COFIDI

1. **Objetivo:** Emisión de comprobantes fiscales.
2. **Fundamento:** Artículo 14, fracción VIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.

- RFC.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E5. Directorio Nacional de Universidades e Instituciones de Educación Superior

1. **Objetivo:** Mantener vínculos con organismos e instituciones públicas y privadas.
2. **Fundamento:** Artículo 14, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Datos académicos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) auxiliar.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E6. Directorio de Medios de Comunicación

1. **Objetivo:** Mantener contacto con medios de comunicación.

2. **Fundamento:** Artículo 14, fracción III del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Teléfono fijo o celular.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Dictaminador(a) II.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

E7. Directorio de la Dirección General

1. **Objetivo:** Exclusivo para efectos laborales.
2. **Fundamento:** Artículo 9, fracciones I y II del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Ocupación.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Vía telefónica.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Secretario(a) particular.
   - Secretario(a) de Director General.

6. **Tipo de soporte**
   - Físico.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE CASAS DE LA CULTURA JURÍDICA

F. Dirección General de Casas de la Cultura Jurídica

F1. Inscripción en la Plataforma Electrónica de Acompañamiento y Seguimiento para el Aprendizaje

1. **Objetivo:** Inscripción en la plataforma para asistir a cursos
2. **Fundamento:** Artículo 37, fracción VII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Ciudad de residencia.
4. **Forma de obtención:**
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de actualización profesional.
   - Titulares de las Casas de la Cultura Jurídica.
   - Encargados de Eventos de las Casas de la Cultura Jurídica.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** En tanto el titular de los datos cancele su inscripción en la plataforma.

F2. Registro Único de Disertantes

1. **Objetivo:** Invitación de disertantes para desarrollar eventos.
2. **Fundamento:** Artículo 37, fracción VII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**

- Nombres y apellidos.
- Correo electrónico.
- Ciudad de residencia.
- Teléfono fijo o celular.
- Ocupación.
- Nivel educativo.
- Curriculum Vitae.
- Datos académicos.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Eventos.
   - Titulares de las Casas de la Cultura Jurídica.
   - Encargados de Eventos de las Casas de la Cultura Jurídica.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: En tanto el titular de los datos cancele su inscripción en la plataforma.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE ESTUDIOS, PROMOCIÓN Y DESARROLLO DE LOS DERECHOS HUMANOS

G. Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos

G1. Protocolos de Actuación

1. **Objetivo:** Fines estadísticos de descarga de los protocolos de actuación en materia de derechos humanos.
2. **Fundamento:** Artículo 39, fracción II del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Correo electrónico.
4. **Forma de obtención:**
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Profesional operativo.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

G2. Registro de participantes cursos virtuales "Acceso a la justicia especializada en niñez y adolescencia" y "Psicología forense en especializada en niñas, niños y adolescentes"

1. **Objetivo:** Seguimiento de participantes de curso virtual y fines estadísticos.
2. **Fundamento:** Artículos 38 y 39, fracciones I, II y XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de Eventos.
   - Titulares de las Casas de la Cultura Jurídica.

- Encargados de Eventos de las Casas de la Cultura Jurídica.

6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación**: 1 año.

G3. Registro de participantes a cursos y talleres presenciales

1. **Objetivo:** Para fines estadísticos.
2. **Fundamento:** Artículos 38 y 39, fracciones I, II y XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Vía telefónica.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad administrativa.
7. **Transferencias**: No.
8. **Plazo de conservación**: 1 año.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE TESORERÍA

H. Dirección General Tesorería

H1. Base de Viáticos

1. **Objetivo:** Para dar trámite a viáticos.
2. **Fundamento:** Artículo 24, fracción II del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Fecha de nacimiento.
4. **Forma de obtención:**
   - Solicitudes de viáticos presentadas por las unidades administrativas que comisionan.
5. **Cargos que tienen acceso a la base de datos:**
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo (Sección RFP; serie: MX-SCJN-RFP-22).
7. **Transferencias**: No.
8. **Plazo de conservación:** 6 años.

H2. Relación de Pagos Electrónicos

1. **Objetivo:** Realizar el pago a proveedores y prestadores de servicios por cheque o transferencia electrónica bancaria.
2. **Fundamento:** Artículo 24, fracción II del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos laborales.
   - Datos bancarios.
4. **Forma de obtención:**
   - Cuentas por liquidar internas generadas por la Dirección General de Presupuesto y Contabilidad.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de Egresos.
   - Jefe(a) de Departamento de Pagos a Proveedores.

6. **Tipo de soporte**
   - Servidor de la institución (sección RFP, serie: MX-SCJN-RFP-22).
   - Archivero de la unidad administrativa.
7. **Transferencias**: No.
8. **Plazo de conservación**: 6 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA SECRETARÍA DE SEGUIMIENTO DE COMITÉS DE PRESTACIONES COMPLEMENTARIAS.

I. Secretaría de Seguimiento de Comités de Prestaciones Complementarias

I1. Tramitación de Solicitudes de Prestaciones Médicas Complementarias Programadas o por Emergencia Médica

1. **Objetivo:** Trámite de la prestación médica complementaria.
2. **Fundamento:** Artículo 24, fracción XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - **Estado de interdicción o incapacidad legal – Sensible.**
   - **Menor de edad – Sensible.**
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Teléfono fijo o celular.
   - **Discapacidad – Sensible.**
   - Circunstancias socioeconómicas.
   - Sexo.
   - Año de nacimiento o edad.
   - Ocupación.
   - **Datos de salud – Sensible.**
   - Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, etc.).
   - **Beneficiarios – Sensible (cuando se trate de menores de edad).**
   - Datos patrimoniales.
   - Antecedentes laborales.
   - Firma.
   - **Huella digital – Sensible.**
   - Datos personales contenidos en documento para acreditar personalidad del representante.
   - Estado civil.

- Datos bancarios.

4. **Forma de obtención:**
   - Escrito presentado en la SSCPC.
5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) de Seguimiento de Comités de Prestaciones Complementarias.
   - Subdirector(a) de Administración de Prestaciones Complementarias.
   - Profesional operativo.
   - Técnico operativo
6. **Tipo de soporte**
   - Archivero de la unidad administrativa.
7. **Transferencias**: Se transfieren los datos para solicitar el pago de la prestación médica complementaria.
   - Nacional Financiera, S.N.C., Institución de Banca de Desarrollo
8. **Plazo de conservación:** 6 años.

I2. Trámite de pago de facturas por la adquisición de artículos promocionales de la SCJN

1. **Objetivo:** Revisar datos fiscales para la emisión de contra-recibo y trámite de pago.
2. **Fundamento:** Artículo 24, fracción XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos laborales.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - RFC.
   - Datos bancarios.
4. **Forma de obtención:**
   - Expreso y por escrito.
5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) de Seguimiento de Comités de Prestaciones Complementarias.
   - Profesional operativo.
   - Técnico operativo.
6. **Tipo de soporte**
   - Archivero de la unidad administrativa.
7. **Transferencias**: Se transfieren los datos para solicitar el pago al proveedor.
   - Nacional Financiera, S.N.C., Institución de Banca de Desarrollo

8. **Plazo de conservación**: 6 años.

I3. Tramitación de Solicitudes de Pensiones Complementarias Mandos Superiores

1. **Objetivo:** Registrar a los beneficiarios de pensiones complementarias a mandos superiores.
2. **Fundamento:** Artículo 24, fracción XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - **Estado de interdicción o incapacidad legal – Sensible.**
   - **Menor de edad – Sensible.**
   - Persona fallecida.
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - **Discapacidad – Sensible.**
   - Sexo.
   - Año de nacimiento o edad.
   - Ocupación.
   - **Beneficiarios – Sensible tratándose de menores de edad.**
   - Datos patrimoniales.
   - Antecedentes laborales.
   - Firma.
   - **Huella digital – Sensible.**
   - Datos personales contenidos en documento para acreditar personalidad del representante.
   - Estado civil.
   - Pensión alimenticia.
   - Datos de contacto.
   - Datos bancarios.
   - RFC.
   - CURP.
4. **Forma de obtención:**

- De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.

5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) de Seguimiento de Comités de Prestaciones Complementarias.
   - Subdirector(a) de Administración de Prestaciones Complementarias.
   - Profesional operativo.
   - Técnico operativo.
6. **Tipo de soporte**
   - Archivero de la unidad administrativa.
7. **Transferencias**: Se transfieren los datos para solicitar el pago de la pensión complementaria.
   - Nacional Financiera, S.N.C., Institución de Banca de Desarrollo
8. **Plazo de conservación**: Durante el tiempo que esté vigente la pensión complementaria.

I4. Tramitación de Solicitudes de Pensiones Complementarias Mando Medio y Personal Operativo

1. **Objetivo:** Registrar a los beneficiarios de pensiones complementarias a mandos medios y personal operativo.
2. **Fundamento:** Artículo 24, fracción XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - **Estado de interdicción o incapacidad legal – Sensible.**
   - **Menor de edad – Sensible.**
   - Persona fallecida.
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - **Discapacidad – Sensible.**
   - Sexo.
   - Año de nacimiento o edad.
   - Ocupación.

- **Beneficiarios – Sensible tratándose de menores de edad.**
- Datos patrimoniales.
- Antecedentes laborales.
- Firma.
- **Huella digital – Sensible.**
- Datos personales contenidos en documento para acreditar personalidad del representante.
- Estado civil.
- Pensión alimenticia.
- Datos de contacto.
- Datos bancarios.
- RFC.
- CURP.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) de Seguimiento de Comités de Prestaciones Complementarias.
   - Subdirector(a) de Administración de Prestaciones Complementarias.
   - Profesional operativo.
   - Técnico operativo.
6. **Tipo de soporte**
   - Archivero de la unidad administrativa.
7. **Transferencias**: Se transfieren los datos para solicitar el pago de la pensión complementaria.
   - Nacional Financiera, S.N.C., Institución de Banca de Desarrollo
8. **Plazo de conservación**: Durante el tiempo que esté vigente la pensión complementaria.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE SERVICIOS MÉDICOS

J. Dirección General de Servicios Médicos

J1. Registro de Pacientes y Expediente Clínico Electrónico

1. **Objetivo:** Registro y Consulta al Expediente Clínico Electrónico.
2. **Fundamento:** Artículo 17, fracciones I y XI del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Sexo.
   - Año de nacimiento o edad.
   - Datos laborales.
   - **Datos de salud – Sensible.**
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) General.
   - Subdirector(a) General.
   - Director(a) de área.
   - Subdirector(a) de área.
   - Profesionales operativos.
   - Técnicos operativos.
   - Técnicos en previsión social.
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo (sección: RH; serie: MX-SCJN-RH-19; subserie: MX-SCJN-RH-19.1).
7. **Transferencias**: No.
8. **Plazo de conservación:** 6 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DEL CENTRO DE ESTUDIOS CONSTITUCIONALES

K. Centro de Estudios Constitucionales

K1. Registro de asistentes a eventos del Centro de Estudios Constitucionales

1. **Objetivo:** Para registro de asistentes al evento.
2. **Fundamento:** Acuerdo Tercero, Fracción V del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
   - Ocupación.
   - Nivel educativo.
   - Teléfono fijo o celular.
4. **Forma de obtención:**
   - Correo electrónico.
   - Vía telefónica.
5. **Cargos que tienen acceso a la base de datos:**
   - Secretario(a) de Director General.
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

K2. Datos de ponentes de eventos para trámite de transportación y hospedaje

1. **Objetivo:** Para solicitar a Tesorería el trámite de transportación y hospedaje.
2. **Fundamento:** Acuerdo Tercero, Fracciones V y X del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Nacionalidad.

- Ocupación.
- Curriculum Vitae.
- Fotografía.
- Fecha de nacimiento.

4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Profesional operativo.
   - Investigador jurisprudencial.
   - Coordinador(a) administrativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

K3. Datos de autores para pago por elaboración de libros y artículos

1. **Objetivo:** Para solicitar a Tesorería el pago por elaboración de libros y artículos.
2. **Fundamento:** Acuerdo Tercero, Fracción X del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Datos bancarios.
   - Fotografía.
   - Firma.
   - CURP o documento de identidad.
   - Lugar y fecha de nacimiento.
   - Datos fiscales.
4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Investigador jurisprudencial.

- Coordinador(a) administrativo.

6. **Tipo de soporte**
   - Equipo de cómputo.
   - Archivero de la unidad administrativa.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

K4. Datos de autores para la autorización de publicación de libros y artículos

1. **Objetivo:** Para obtener la cesión de derechos de los autores a favor de la Suprema Corte de Justicia de la Nación para la publicación de libros y artículos.
2. **Fundamento:** Acuerdo Tercero, Fracción X del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Fotografía.
   - Domicilio.
   - Teléfono fijo o celular.
   - Firma.
4. **Forma de obtención:**
   - Correo electrónico.
   - Presencia física del titular de los datos personales.
5. **Cargos que tienen acceso a la base de datos:**
   - Investigador jurisprudencial.
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
   - Archivero de la unidad administrativa.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

K5. Datos de autores para publicación en el Blog y de personas interesadas en publicar en la sección de comentarios de la página web del Centro de Estudios Constitucionales

1. **Objetivo:** Comunicar a las personas la publicación en el blog de su texto o comentario.
2. **Fundamento:** Acuerdo Tercero, Fracciones III y VI del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.

- Correo electrónico.

4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Investigador jurisprudencial.
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

K6. Datos de personas para publicación en Foro de debate de la página web del Centro de Estudios Constitucionales

1. **Objetivo:** Comunicar a las personas la publicación de sus comentarios en el Foro de discusión.
2. **Fundamento:** Acuerdo Tercero, Fracciones III y IX del Estatuto del Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Investigador jurisprudencial.
   - Profesional operativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DEL CENTRO DE DOCUMENTACIÓN Y ANÁLISIS, ARCHIVOS Y COMPILACIÓN DE LEYES

L. Centro de Documentación y Análisis, Archivos y Compilación de Leyes

L1. Atención a personas privadas de su libertad

1. **Objetivo:** Para registrar las consultas de personas privadas de su libertad y elaborar estadísticas sobre los servicios proporcionados.
2. **Fundamento:** Artículo 147, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
4. **Forma de obtención:**
   - Escrito o formato enviado por mensajería.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Jefe de departamento.
   - Profesional operativo.
6. **Tipo de soporte**
   - Servidor de la institución.
   - Archiveros de la unidad administrativa (sección: AAD; serie: MX-SCJN-AAD-5).
7. **Transferencias**: No.
8. **Plazo de conservación:** 6 años.

L2. Búsqueda y préstamo de expedientes judiciales

1. **Objetivo:** Identificación y control de préstamo de expedientes judiciales.
2. **Fundamento:** Artículo 147, fracción I del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Firma.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.

- Vale de préstamo.

5. **Cargos que tienen acceso a la base de datos:**
   - Técnico operativo.
6. **Tipo de soporte**
   - Equipo de cómputo.
   - Archiveros de la unidad administrativa (sección AAD; serie: MX-SCJN-AAD-05; subserie: MX-SCJN-AAD-05.04).
7. **Transferencias**: No.
8. **Plazo de conservación:** 10 años.

L3. Control de acceso a inmuebles

1. **Objetivo:** registro de acceso a personas, vehículos y empresas.
2. **Fundamento:** Artículo 147, fracción XIII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
   - Teléfono fijo o celular.
4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) general.
   - Coordinador(a) administrativo.
   - Profesional operativo.
   - Secretaria.
6. **Tipo de soporte**
   - Equipo de cómputo.
   - Archivero de la unidad administrativa (sección: SS; serie: MX-SCJN-SS-11; subserie: MX-SCJN-SS-11.1, MX-SCJN-SS-11.2 y MX-SCJN-SS-11.3).
7. **Transferencias**: No.
8. **Plazo de conservación:** 6 años.

L4. Servicio del sistema bibliotecario

1. **Objetivo:** Creación de perfil del usuario y elaboración de estadísticas de los servicios proporcionados.
2. **Fundamento:** Artículo 147, fracción X del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Año de nacimiento o edad.
   - Correo electrónico.
   - Firma.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Jefe(a) de departamento.
   - Profesional operativo.
   - Técnico operativo.
6. **Tipo de soporte**
   - Servidor de la institución.
   - Archivero de la unidad administrativa (sección: AAD; serie: MX-SCJN-AAD-05; subserie: MX-SCJN-AAD-05.04).
7. **Transferencias**: No.
8. **Plazo de conservación:** 6 años.

L5. Servicio de consulta de acervo legislativo

1. **Objetivo:** Registrar las consultas al acervo legislativo y generar estadísticas.
2. **Fundamento:** Artículo 147, fracción IX del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.

- Jefe(a) de departamento.

6. **Tipo de soporte**
   - Servidor de la institución.
   - Archivero de la unidad administrativa (sección: AAD; serie: MX-SCJN-AAD-05).
7. **Transferencias**: No.
8. **Plazo de conservación:** 1 año.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA COMISIÓN SUBSTANCIADORA ÚNICA DEL PODER JUDICIAL DE LA FEDERACIÓN

M. Comisión Substanciadora única del Poder Judicial de la Federación

M1. Acuerdos, notificaciones y resoluciones

1. **Objetivo:** Dictar acuerdos, practicar notificaciones, emitir resoluciones, emitir dictámenes en conflictos de trabajo de la competencia del Pleno de la Suprema Corte de Justicia de la Nación;
2. **Fundamento:** Artículo 123, Apartado B, Fracción XII, segundo párrafo constitucional y 152 a 161 de la Ley Federal de los Trabajadores al Servicio del Estado.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Circunstancias socioeconómicas.
   - Domicilio.
   - **Datos de salud – Sensible.**
   - Año de nacimiento o edad.
   - Persona fallecida.
   - Datos laborales.
   - Firma.
   - Sexo.
   - Nacionalidad.
   - Descuentos personales.
   - Antecedentes laborales.
   - Datos sindicales.
   - Beneficiarios.
   - Datos personales contenidos en documento para acreditar personalidad del representante.
   - Estado civil.
   - **Motivos de licencia en el trabajo – Sensible.**
   - **Causas de inasistencia al trabajo – Sensible.**
   - Relación de parentesco o civil.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Correo electrónico.

- Por escrito presentado directamente en la Comisión Substanciadora Única del Poder Judicial de la Federación.
- Por escrito enviado por mensajería.

5. **Cargos que tienen acceso a la base de datos:**
   - Tercer(a) Integrante y Presidente(a) de la Comisión Substanciadora Única del Poder Judicial de la Federación.
   - Representante de la Suprema Corte de Justicia de la Nación.
   - Representante del Sindicato de Trabajadores del Poder Judicial de la Federación.
   - Secretarios.
   - Persona operativo.
6. **Tipo de soporte**
   - Archiveros de la unidad administrativa.
   - Fuentes de acceso público (portal e intranet).
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE PRESUPUESTO Y CONTABILIDAD

N. Dirección General de Presupuesto y Contabilidad

N1. Solicitud de Pagos

1. **Objetivo:** Elaborar propuestas de pago para entregar recursos a los beneficiarios;
2. **Fundamento:** Artículo 23 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Firma.
   - RFC
   - Datos bancarios.
   - INE.
4. **Forma de obtención:**
   - Correo electrónico.
   - Oficios.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector de área.
   - Profesionales operativos.

6. **Tipo de soporte**
   - Archiveros de la unidad administrativa.
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

N2. Catálogo de acreedores

1. **Objetivo:** Mantener actualizada la base datos para efectuar pagos;
2. **Fundamento:** Artículo 23 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - RFC.
   - CURP.
   - Datos bancarios.
4. **Forma de obtención:**
   - Correo electrónico.
   - Oficios.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesionales operativos.
6. **Tipo de soporte**
   - Archiveros de la unidad administrativa.
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

N3. Guarderías

1. **Objetivo:** Elaborar propuestas de pago para entregar recursos a los beneficiarios;
2. **Fundamento:** Artículo 23 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - **Menor de edad – Sensible.**
   - Nivel educativo.
   - CURP.
   - Datos bancarios.

4. **Forma de obtención:**
   - Correo electrónico.
   - Oficios.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesionales operativos.
6. **Tipo de soporte**
   - Archiveros de la unidad administrativa.
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

N4. Catálogo de firmas

1. **Objetivo:** Para la consulta y verificación, por parte del personal de la Dirección General de Presupuesto y Contabilidad, de las firmas y rúbricas de los servidores públicos autorizados para realizar trámites presupuestales;
2. **Fundamento:** Artículo 23 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Firma.
   - Rúbrica.
4. **Forma de obtención:**
   - Oficio o formato.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) General de Presupuesto y Contabilidad.
   - Subdirector(a) General de Presupuesto.
   - Subdirector(a) General de Contabilidad.
   - Subdirector(a) General de Normativa y Seguimiento Presupuestal.
   - Director(a) de Presupuesto.
   - Director(a) del Ejercicio del Gasto.
   - Director(a) de Informática.
   - Director(a) de Seguimiento y Administración Documental.
   - Subdirector(a) de Integración Documental.
   - Subdirector(a) de Modificaciones Presupuestales.
   - Subdirector(a) de Servicios Generales e Inversión.
   - Subdirector(a) de Servicios Personales y Obra Pública.

- Subdirector(a) de Contabilidad Financiera.
- Subdirector(a) de Contabilidad Presupuestal y Fideicomisos.
- Subdirector(a) de Informes Presupuestales.
- Subdirector(a) de Contabilidad de Nóminas y Obras.
- Jefe(a) de Departamento de Servicios Personales y Adecuaciones Presupuestales
- Jefe(a) de Departamento de Fondos Fijos, Pago a Proveedores y Viáticos
- Jefa de Departamento de Control Presupuestal
- Jefa de Departamento de Nóminas y Obra Pública
- Jefa de Departamento de Honorarios
- Jefa de Departamento de Control y Registro de Casas de la Cultura Jurídica
- Secretaria de Director General
- 10 Profesionales Operativos de la Subdirección General de Presupuesto
- 8 Profesionales Operativos de la Subdirección General de Contabilidad
- Profesional Operativo de la Dirección de Seguimiento y Administración Documental

6. **Tipo de soporte**
   - Archiveros de la unidad administrativa (RFP-17-10).
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE INFRAESTRUCTURA FÍSICA

O. Dirección General de Infraestructura Física

O1. Catálogo referencial de contratistas

1. **Objetivo:** Tener una relación de Personas Físicas o Morales, que se encuentren inscritas o les interese inscribirse en el Catálogo referencial de Contratistas y sean invitados en los Procedimientos de Contratación;
2. **Fundamento:** Artículo 23 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Domicilio.
   - Correo electrónico.
   - Curriculum Vitae.
   - Antecedentes laborales.
   - Datos personales contenidos en documento para acreditar personalidad del representante.
4. **Forma de obtención:**
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Subdirector(a) de área.
   - Profesionales operativos.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** No especifica.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE SEGURIDAD

P. Dirección General de Seguridad

P1. Registro de entrada

1. **Objetivo:** Registro de las personas que acceden a los inmuebles de la SCJN;
2. **Fundamento:** Artículo 28 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
5. **Cargos que tienen acceso a la base de datos:**
   - Técnicos de seguridad.
6. **Tipo de soporte**
   - Servidor de la institución.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

P2. Circuito cerrado de televisión

1. **Objetivo:** Registrar vídeo para seguridad interna;
2. **Fundamento:** Artículo 28 del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Información descriptiva sobre la fisonomía y características físicas de las imágenes de las personas.
4. **Forma de obtención:**
   - Registro de Videograbación de CCTV.
5. **Cargos que tienen acceso a la base de datos:**
   - Técnicos de seguridad.
6. **Tipo de soporte**
   - Área de CCTV.
7. **Transferencias**: No.
8. **Plazo de conservación:** 90 días.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA UNIDAD GENERAL DE TRANSPARENCIA Y SISTEMATIZACIÓN DE LA INFORMACIÓN JUDICIAL

Q. Unidad General de Transparencia y Sistematización de la información judicial

Q1. Servicio social

1. **Objetivo:** Contar con el registro de las personas que realizan el servicio social en dicha unidad;
2. **Fundamento:** Artículo 42 del Reglamento Orgánico en Materia de Administración de la SCJN.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Nivel educativo.
   - Curriculum vitae.
   - Datos académicos.
   - Antecedentes laborales.
4. **Forma de obtención:**
   - Escrito o formato presentado.
5. **Cargos que tienen acceso a la base de datos:**
   - Coordinador(a) administrativa.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 4 años.

Q2. Resultados de evaluaciones psicométricas

1. **Objetivo:** Contar con el registro de las personas que realizan el servicio social en dicha unidad;
2. **Fundamento:** Artículo 42 del Reglamento Orgánico en Materia de Administración de la SCJN.

3. **Datos personales que se encuentran en el sistema:**
   - **Resultados de evaluación psicométrica – Sensible.**
4. **Forma de obtención:**
   - Informe enviado por la DGRH.
5. **Cargos que tienen acceso a la base de datos:**
   - Coordinador(a) administrativa.
6. **Tipo de soporte**
   - Archivero de la unidad.
7. **Transferencias**: No.
8. **Plazo de conservación:** 4 años.

Q3. Formato de procedimiento sumario

1. **Objetivo:** enviar información solicitada y generar estadísticas;
2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q4. Formato de procedimiento ordinario

1. **Objetivo:** enviar información solicitada y generar estadísticas;

2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
   - Domicilio.
   - Teléfono fijo o celular.
   - **Lengua indígena – sensible.**
   - Persona fallecida.
   - Sexo.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Datos laborales.
   - **Pertenencia a pueblo indígena – sensible.**
   - Firma.
   - **Datos de salud – sensible.**
   - Datos académicos.
   - Creencias religiosas, filosóficas o morales.
   - Información migratoria.
   - **Origen étnico o racial – sensible.**
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q5. Consulta física y electrónica de expedientes

1. **Objetivo:** enviar información solicitada y generar estadísticas;
2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q6. Formatos de procedimiento de acceso a la justicia

1. **Objetivo:** enviar información solicitada y generar estadísticas;
2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.

- Equipo de cómputo.

7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q7. Recibos de pago

1. **Objetivo:** enviar información solicitada y generar estadísticas;
2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Vía telefónica.
   - Correo electrónico.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q8. Solicitudes de personas privadas de su libertad

1. **Objetivo:** enviar información solicitada y generar estadísticas;
2. **Fundamento:** Artículo 42, fracciones IV, V y VIII del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Correo electrónico.
   - Domicilio.

- Teléfono fijo o celular.
- **Lengua indígena – sensible.**
- Persona fallecida.
- Sexo.
- Nacionalidad.
- Ocupación.
- Nivel educativo.
- Datos laborales.
- **Pertenencia a pueblo indígena – sensible.**
- Firma.
- **Datos de salud – sensible.**
- Datos académicos.
- Creencias religiosas, filosóficas o morales.
- Información migratoria.
- **Origen étnico o racial – sensible.**

4. **Forma de obtención:**
   - Por correo postal
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector(a) de área.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

Q9. Atención ciudadana

1. **Objetivo:** Dar contestación a las peticiones elaboradas por el público en general y que son dirigidas al Presidente de la SCJN;
2. **Fundamento:** Artículo 42, fracción XIX del Reglamento Orgánico en Materia de Administración.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.

- Entidad Federativa.
- **Persona privada de su libertad – Sensible.**

4. **Forma de obtención:**
   - Correo electrónico.
   - Correspondencia.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) de área.
   - Jefa de departamento.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS Y DE REGISTRO PATRIMONIAL.

R. Dirección General de Responsabilidades Administrativas y de Registro Patrimonial

R1. Recepción de declaraciones patrimoniales y de Intereses

1. **Objetivo:** Llevar el seguimiento de la evolución y la verificación de la situación patrimonial de los Declarantes, en los términos de la presente LGRA;
2. **Fundamento:** 108, párrafos primero y quinto de la Constitución Política de los Estados Unidos Mexicanos; 11, fracción XIII y 222 de la Ley Orgánica del Poder Judicial de la Federación; 32, 33, 35, 39 y 46 de la Ley General de Responsabilidades Administrativas; 51 y 52 del Acuerdo General Número 9/2005 del Pleno de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - CURP.
   - RFC.
   - Sexo
   - Estado civil.
   - Lugar de nacimiento.
   - Nacionalidad.
   - Tipo de vivienda.
   - Domicilio.
   - Teléfono fijo o celular.
   - Correo electrónico.
   - Datos laborales.
   - Nivel educativo.
   - Estado de los estudios.
   - Títulos y constancias profesionales.
   - Número de cédula profesional.
   - Datos académicos.
   - Información curricular adicional.
   - Salario del servidor público.
   - Ingreso anual o mensual netos.
   - Otros ingresos por actividad industrial y/o comercial.
   - Otros ingresos por intereses, rendimientos o beneficios generados en cuentas de ahorro de inversiones, etc.

- Otros ingresos por servicios profesionales, participación en consejos, consultorías o asesorías, etc.
- Otros ingresos por arrendamientos, regalías, sorteos, concursos, venta de valores, donaciones, herencias o legados, pensión alimenticia, etc.
- Ingresos de su cónyuge, concubina o concubinario.
- Ingresos de sus dependientes económicos.
- Saldo a favor del ISR recibido.
- Bienes inmuebles y datos de la operación.
- Bienes muebles y datos de la operación.
- Donaciones de dinero.
- Inversiones, cuentas bancarias y ahorro.
- Gravámenes o adeudos.
- **Datos de cónyuge, concubina o concubinario y dependiente económicos – sensible.**
- Firma.

4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Internet o sistema informático.
   - Escrito o formato enviado a la DGRARP por mensajería.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) general.
   - Director(a) de área.
   - Dictaminador(a).
   - Subdirector(a) de área.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Servidor de la institución.
7. **Transferencias**: Sí, que la autoridad solicitante pueda cumplir con sus funciones jurisdiccionales.
   - Juzgados.
   - Ministerios públicos.
8. **Plazo de conservación:** 12 años.

R2. Expedientes de responsabilidad administrativas

1. **Objetivo:** Recibir quejas y denuncias, substanciar procedimientos de responsabilidad administrativa, mantener actualizado el registro de servidores públicos sancionados;
2. **Fundamento:** Artículo 33, fracciones VII, VIII, IX y X del Reglamento Orgánico en Materia de Administración de la SCJN.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - **Menor de edad – sensible.**
   - Persona fallecida.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - **Discapacidad – sensible.**
   - Sexo.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Curriculum vitae.
   - Descuentos personales.
   - **Beneficiarios – sensible.**
   - Firma.
   - Huella dactilar.
   - Títulos profesionales.
   - Antecedentes laborales.
   - Datos académicos.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Correo electrónico.
   - Por escrito con el que se presenta queja o denuncia.
   - Por transferencia.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) general.
   - Subdirector(a) general.
   - Profesional operativo.
6. **Tipo de soporte**

- Archivero de la unidad.
- Equipo de cómputo.

7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

R3. Expedientes de Inconformidades

1. **Objetivo:** Trámite del recurso de inconformidad;
2. **Fundamento:** Artículo 189 del Acuerdo General de Administración VI/2008.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Curriculum vitae.
   - Firma.
   - Huella dactilar.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Por escrito.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) general.
   - Subdirector(a) general.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

R4. Expedientes de Conciliaciones

1. **Objetivo:** Intervención en los procedimientos de conciliación;
2. **Fundamento:** Artículo 188 del Acuerdo General de Administración VI/2008.
3. **Datos personales que se encuentran en el sistema:**
   - Nombre y apellidos.
   - Datos personales contenidos en la identificación oficial presentada por la persona física.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Sexo.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
   - Curriculum vitae.
   - Firma.
   - Huella dactilar.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales.
   - Por escrito.
5. **Cargos que tienen acceso a la base de datos:**
   - Director(a) general.
   - Subdirector(a) general.
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.
7. **Transferencias**: No.
8. **Plazo de conservación:** Permanente.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA UNIDAD GENERAL DE INVESTIGACIÓN DE RESPONSABILIDADES ADMINISTRATIVAS

S. Unidad General de Investigación de Responsabilidades Administrativas

S1. Procedimiento de Investigación de Responsabilidad Administrativa

1. **Objetivo:** Acreditar la identidad de los involucrados (persona física) en el desahogo de la investigación;
2. **Fundamento:** Artículo 9, fracción XVI y 45, fracción XII del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Domicilio.
   - Correo electrónico.
   - Firma.
   - Teléfono fijo o celular.
   - Año de nacimiento o edad.
   - Antecedentes laborales.
   - Sexo.
4. **Forma de obtención:**
   - De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.
   - Por correo electrónico, enviado por las personas involucradas en la investigación.
   - Por escrito, presentado ante esta Unidad o bien ante la Contraloría, la Dirección General de Responsabilidades y Registro Patrimonial o ante la Presidencia de este Alto Tribunal.
   - Por escrito enviado por paquetería a esta Unidad bien ante la Contraloría, Dirección General de Responsabilidades y Registro Patrimonial o ante la Presidencia de este Alto Tribunal.
5. **Cargos que tienen acceso a la base de datos:**
   - Dictaminador(a).
   - Profesional operativo.
6. **Tipo de soporte**
   - Archivero de la unidad.
   - Equipo de cómputo.

7. **Transferencias**: No.
8. **Plazo de conservación:** 5 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS.

T. Dirección General de Asunto Jurídicos

T1. Tramitación de juicios, medios de defensa, responsabilidades administrativas, opiniones jurídicas y propiedad intelectual

1. **Objetivo:** Tramitación de juicios, medios de defensa, responsabilidades administrativas, opiniones jurídicas y propiedad intelectual;
2. **Fundamento:** Artículo 35, fracciones II, III, IX, XXI, del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Datos personales contenidos en la identificación oficial presentada por la persona física laborales.
4. **Forma de obtención:**
   - Oficios y escritos.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector General de lo Contencioso y Normativa.
   - Director de Juicios y Medios de Defensa.
   - Director de Apoyo a la Normativa y Asuntos de Propiedad Intelectual.
   - Director de Consultas Administrativas.
   - Subdirector de área.
   - Profesional operativo.
6. **Tipo de soporte:**
   - Archivero de la unidad.
7. **Transferencias**: Sí, Intervenir en los asuntos en los que la SCJN es parte:
   - Ministerios públicos.
   - Juzgados.
   - Instituto Nacional del Derecho de Autor.
   - Instituto Mexicano de Propiedad Intelectual.
8. **Plazo de conservación:** 6 y 12 años.

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

DE LA SECRETARÍA GENERAL DE LA PRESIDENCIA

U. Secretaría General de la Presidencia

U1. Atención Ciudadana

1. **Objetivo:** Dar trámite a las solicitudes de los ciudadanos en ejercicio del derecho de petición y proporcionar la orientación adecuada;
2. **Fundamento:** Artículo 10 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.
3. **Datos personales que se encuentran en el sistema:**
   - Nombres y apellidos.
   - Menor de edad.
   - Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer.
   - Domicilio.
   - Correo electrónico.
   - Teléfono fijo o celular.
   - Discapacidad.
   - Sexo.
   - Pertenencia a un pueblo indígena.
   - Circunstancias socioeconómicas.
   - Año de nacimiento o edad.
   - Nacionalidad.
   - Ocupación.
   - Nivel educativo.
4. **Forma de obtención:**
   - Oficios y escritos.
5. **Cargos que tienen acceso a la base de datos:**
   - Subdirector General de lo Contencioso y Normativa.
   - Director de Juicios y Medios de Defensa.
   - Director de Apoyo a la Normativa y Asuntos de Propiedad Intelectual.
   - Director de Consultas Administrativas.
   - Subdirector de área.
   - Profesional operativo.
6. **Tipo de soporte:**

- Archivero de la unidad administrativa.
- Equipo de cómputo.

7. **Transferencias**: No.
8. **Plazo de conservación:** 12 años.

ANEXO 3. Nota Informativa sobre el aviso de privacidad

- **Racionalidad del Aviso de Privacidad**

De conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el aviso de privacidad es el documento a disposición del titular de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos (artículo 3, fracción II).

El uso del aviso de privacidad en los sujetos obligados tiene como finalidad contar con un instrumento adecuado que permita, por un lado, cumplir con el principio constitucional de informar a los titulares, la existencia y características principales del tratamiento al que serán sometidos sus datos personales; y por otro lado, para que los titulares puedan tomar decisiones informadas respecto a dichos tratamientos (artículo 26).

El aviso de privacidad es unos de los medios idóneos para materializar la protección de datos personales, en tanto las personas tienen el derecho a decidir sobre el uso que puede dárseles a de manera expresa o tácita. Es expreso cuando la voluntad del titular se manifieste verbalmente sus datos.

El consentimiento informado, de conformidad con los parámetros de la LGPDPPSO, puede otorgarse, por escrito, medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. Sin embargo, en el consentimiento expreso se debe verificar que éste se otorgó de manera informada y se pueda comprobar de manera indubitable; es decir, que el titular supo de manera anticipada el tipo de tratamiento a que sus datos serían sometidos, los medios a través de los cuáles podía oponerse a dicho tratamiento, el nombre del responsable, entre otros (artículo 21).

Es por lo anterior que la propia LGPDPPSO reconoce que el consentimiento también puede otorgarse de manera tácita, cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario (artículo 21). Esto es así, ya que el aviso de privacidad contiene todos los elementos necesarios para que pueda considerarse que un consentimiento se otorgó de manera informada.

Por regla general, el consentimiento tácito es válido, salvo que la ley requiere la obtención del consentimiento expreso (artículo 21). Es necesario el consentimiento expreso cuando

se recaben datos personales sensibles (datos de menores de edad, estado de salud, datos biométricos, preferencias sexuales, políticas o religiosas, entre otros).

- **Elementos del Aviso de Privacidad**

El aviso de privacidad debe caracterizarse por ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible y con una estructura y diseño que facilite su entendimiento, ateniendo al perfil de los titulares a quien irá dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente.

De conformidad con los parámetros en la materia, el aviso de privacidad se deberá poner a disposición del titular en dos modalidades: simplificado e integral. El primero tiene como finalidad contar con un documento sencillo, claro y concreto, en donde se le dote al titular, de primera mano y en el momento en que se recaban sus datos, de la información básica respecto al tratamiento a que serán sometidos sus datos personales. El aviso de privacidad simplificado debe contener la siguiente información (artículo 27):

I. La denominación del responsable;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales.
III. Los mecanismos y medios disponibles para que el titular, en su caso pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieran el consentimiento del titular, y
IV. El sitio donde se podrá consultar el aviso de privacidad integral.

Por su parte, el aviso de privacidad integral es el documento con todos los elementos necesarios para que el titular de los datos personales se informe de manera completa sobre el tratamiento y la manera en que puede ejercer su derecho de protección de datos personales. Éste debe estar publicado de manera permanente en el sitio o medio que se informe el aviso de privacidad simplificado, a efecto de que el titular pueda consultarlo en cualquier momento. Este aviso de privacidad debe contar con los siguientes elementos, además de los previstos para el aviso de privacidad simplificado (artículo 28):

I. El domicilio del responsable;
II. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles;
III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales;
V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos de acceso, rectificación, cancelación y oposición;[3]
VI. El domicilio de la Unidad de Transparencia, y
VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios del aviso de privacidad.

- **Medios de difusión del Aviso de Privacidad**

El aviso de privacidad podrá difundirse, poner a disposición del titular o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación. El responsable debe ubicar el aviso de privacidad en un lugar visible que facilite la consulta del titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación (artículo 26).

Sin embargo, los medios de difusión deben correlacionarse con el momento en que debe ponerse a disposición el aviso de privacidad a los titulares, y el tipo de modalidad en que se pone a disposición.

Por ejemplo, el aviso de privacidad simplificado cuenta con una estructura sencilla y concreta, con la finalidad de ponerse a disposición de los titulares en el momento en que se recaban sus datos personales de manera presencial, sin que esto impida que el responsable pueda dar a conocer el aviso de privacidad integral desde un inicio si lo prefiere. Este tipo de aviso de privacidad se usa, generalmente, cuando los datos personales son recabados para otorgar algún servicio o las personas se inscriben a cursos de manera presencial.

El aviso de privacidad simplificado puede ponerse a disposición de manera física, en algún lugar visible del sitio en donde se recaban los datos personales, para que pueda ser mostrado a los titulares a fin de recabar su consentimiento tácito.

En caso de que se requiera el consentimiento expreso, el aviso de privacidad simplificado puede presentarse de manera personalizada al momento de recabarse los datos

[3] De acuerdo con el artículo 43 de la LGPDPPSO, los titulares o sus representantes tienen derecho a solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen. Para profundizar sobre los mismos, consultar los artículos 43 a 47 de la LGPDPPSO.

personales, y destinar un espacio para que el titular pueda firmarlo en señal de que consciente que sus datos personales sean tratados para la finalidad que se expresa en el mismo.

Por su parte, el aviso de privacidad integral deberá estar publicado permanentemente en el sitio o medio que se destine para que pueda ser consultado cuando así lo deseen los titulares. Es recomendable que el aviso de privacidad integral esté publicado en el portal de internet en donde el responsable destine la información relacionada con el tratamiento de los datos personales.

De esta manera, la puesta a disposición de los avisos de privacidad simplificado e integral, se complementan y garantizan que el titular de los datos personales esté debidamente informado y pueda ser recabado su consentimiento en la forma que así se requiera.

ANEXO 4. Medidas de seguridad y análisis de riesgo de datos personales

1. Presentación

El presente documento de referencia se elaboró por la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTSIJ) y tiene como finalidad dotar de herramientas necesarias a las áreas de la Suprema Corte para responder la *Encuesta sobre análisis de riesgo y medidas de seguridad*.

Para lo anterior, se ofrecen algunas aproximaciones al tema de medidas de seguridad en materia de protección de datos personales, cuya referencia son los estándares reconocidos en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO).

En principio y a través del análisis de los conceptos básicos que inciden alrededor del tema, se explica la importancia de las medidas de seguridad en los sujetos obligados y el papel que juegan en la protección de las bases de datos personales. Posteriormente se profundiza en los tipos de medidas de seguridad, categorización de datos y análisis de riesgo.

A partir de este documento orientador, la UGTSIJ desarrolla y aproxima elementos objetivos para continuar con la implementación de las disposiciones legales en la materia, particularmente para la recopilación de los insumos necesarios para el desarrollo del Documento de Seguridad de este Alto Tribunal, bajo los parámetros del artículo 35 de la Ley.

Además, los trabajos en este rubro ayudarán a sensibilizar a las personas involucradas con el tratamiento de los datos personales sobre los parámetros de seguridad y uso adecuado de los mismos, garantizando la confidencialidad y los derechos de protección de los datos personales de los titulares, y las áreas podrán reconocer el estatus que guardan sus tratamientos de datos personales en relación al estándar idóneo de medidas de seguridad que deberían adoptar.

2. Conceptos Básicos

2.1. Bases de datos personales.

Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

A partir de esta definición, es importante analizar los tres elementos que se integran para considerar una base de datos en esos términos:

- Datos personales ordenados de personas físicas identificadas o identificables;
- Condicionados a criterios determinados de ordenación y tratamiento. Es decir, que la recopilación de los datos personales en una base determinada tenga como propósito cumplir alguna finalidad relacionada con las atribuciones del responsable. Esta ordenación se relaciona con la forma de almacenamiento de los mismos; y,
- No depende de la forma en que se crea o se encuentre almacenada, ni por el tipo de soporte, procesamiento u organización para considerarse como tal.

Estos tres elementos son la guía para considerar las bases de datos en posesión de los responsables y definir parámetros sobre su tratamiento.

Sobre la identificación de bases de datos, la UGTSIJ ha trabajado con las áreas administrativas para la creación del *Inventario de Tratamientos de Datos Personales*, que ha permitido identificar las bases de datos personales que poseen.

2.2. Principios y deberes.

Los deberes legales en materia de datos personales deben entenderse a partir de los principios que son la guía para su tratamiento, el cual debe sujetarse a los siguientes estándares:

- Licitud: sujetarse a las facultades y atribuciones que la normatividad aplicable le confiera al sujeto obligado.
- Finalidad: estar justificado.
- Lealtad: los datos personales deben recabarse de manera legítima, garantizando su protección y privacidad.

- Consentimiento: se deberá contar con el consentimiento del titular de los datos personales en caso de que éste sea necesario recabarse.
- Calidad: los datos personales deben ser exactos, correctos, completos y actualizados, a fin de que no se altere la veracidad de éstos.
- Proporcionalidad: solo debe ser de aquellos datos personales adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
- Información: se deberá informar al titular que sus datos personales serán tratados y explicar la finalidad de éste.
- Responsabilidad: los responsables del tratamiento de los datos personales adoptarán las medidas necesarias para garantizar su protección.

Así, los deberes legales apuntalan la protección de los datos personales a través de la implementación de medidas de seguridad y la garantía de confidencialidad de los mismos.

De conformidad con la garantía de confidencialidad, los responsables del tratamiento de datos personales tienen el deber de no divulgar, no poner a disposición de terceros, ni emplear datos personales para otros propósitos que no sean aquellos para los cuales se obtuvieron.

2.3. Medidas de seguridad y sus finalidades

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales[4] y deben conjugarse con el nivel de protección que requieren las bases de datos. Por ejemplo, el nivel de protección será mayor cuando se trate de bases de datos que resguarden datos personales sensibles y/o almacenen información de una gran cantidad de titulares.

La finalidad de las medidas de seguridad es garantizar, con mecanismos tangibles, la protección de los datos personales en todas las áreas donde se tratan.

3. Medidas de seguridad, categorización de datos y riesgo latente.

3.1. Tipos

[4] Artículo 3 fracción XX de la LGPDPPSO

Las medidas de seguridad *administrativas* son las políticas y procedimientos para la gestión, soporte, 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.

Por su parte, las medidas de seguridad *físicas* se refieren a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor. Se deben considerar, entre otras, las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Finalmente, las medidas de seguridad *técnicas* son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir que 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 para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

3.2. Categorización de datos.

Uno de los métodos para determinar el nivel de medidas de seguridad que deben adoptarse en cada base de datos, es conocer la categoría de los datos personales que

albergan cada uno de éstas. A continuación se detallan algunos parámetros de clasificación aceptados:

- *Datos identificativos:* El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos;
- *Datos electrónicos:* Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;
- *Datos laborales*: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;
- *Datos patrimoniales*: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos;
- *Datos sobre procedimientos administrativos*: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio, demás análogos;
- *Datos académicos:* Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos;
- *Datos de tránsito y movimientos migratorios*: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria, y demás análogos;
- *Datos sobre la salud:* El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona, y demás análogos;
- *Datos biométricos:* huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos; y,
- *Datos especialmente protegidos (sensibles):* en algunos casos los datos biométricos arriba señalados, origen étnico o racial, características morales o emocionales,

ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; así como los datos de niños y niñas y demás análogos.

Es necesario advertir que algunos tipos de datos arriba mencionados son susceptibles de hacerse públicos, cuando por ley exista una obligación de difundirlos y/o se trate de servidores públicos, tal es el caso de algunos datos identificativos, patrimoniales, laborales, académicos, etcétera.

3.3. Niveles de riesgo

Las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello, es necesario calcular 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.

A partir del tipo de dato es posible reconocer el factor de riesgo inherente, como se muestra a continuación:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; sobre la salud; biométricos.	Alto	3
Datos especialmente protegidos (sensibles).	Muy alto.	4-5

Al riesgo inherente, es necesario sumarle el volumen de titulares contenidos en la base de datos, por ejemplo:

- Menos de 100 titulares (>100).
- Menos de 1000 titulares (>1000).
- Menos de 10,000 (>10,000)
- Más de 10,000 (<10,000).

El riesgo inherente más el volumen de titulares, da como resultado el nivel de riesgo por tipo de dato:

NIVEL DE RIESGO POR TIPO DE DATO				
Tipo de dato/Número de titulares.	>100	>1000	>10,000	<10,000
Datos especialmente protegidos (sensibles).	4	4	5	5
Datos de tránsito y movimientos migratorios; sobre la salud; biométricos.	1	2	3	3
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	1	1	2	2
Datos identificativos.	1	1	1	1

Fuente: "Metodología de análisis de riesgo", IFAI, 2014.

El nivel de riesgo por tipo de dato servirá para determinar los controles que se deben considerar para su protección.

Por otra parte, el riesgo por *tipo de acceso* se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro entre mayor sea la accesibilidad, mayor riesgo existe para la información.

ACCESIBILIDAD (CANTIDAD DE ACCESOS)
>10
>20
>30
>40

Finalmente, en el riesgo por *tipo de entorno* este factor representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad.

En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

ENTORNO	NIVEL DE RIESGO
Físico	1
Equipo de cómputo	2
Nube	3
Internet	4

La combinación de los tres factores analizados da como resultado el nivel de riesgo latente de cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

Una vez que se calcula el nivel de riesgo latente por cada tratamiento de datos personales, es posible realizar estrategias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos.

4. Propósito del análisis de riesgo.

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar el nivel de medidas de seguridad que deben ser implementadas para la protección de los datos personales.

Una vez identificado el ideal de medidas de seguridad que deberían implementarse, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un *análisis de brecha,* con el cual resulta posible construir planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación, elementos que conforman el *Documento de Seguridad* de este Alto Tribunal.

ANEXO 5. Encuesta sobre análisis de riesgos y medidas de seguridad

Área:
Tipo de tratamiento:

PRIMERA PARTE Riesgo por tipo de dato

1. Seleccione todas las categorías de datos personales que trata.

Datos identificativos	
Datos electrónicos	
Datos laborales	
Datos patrimoniales	
Datos sobre procedimientos administrativos	
Datos académicos	
Datos de tránsito y movimientos migratorios	
Datos sobre la salud	
Datos biométricos	
Datos especialmente protegidos (sensibles)	

2. Seleccione el volumen de titulares (personas) que conforman la base de datos.

Menos de 100 titulares	
Menos de 1000 titulares	
Menos de 10,000 titulares	
Más de 10,000 titulares	

SEGUNDA PARTE Riesgo por tipo de acceso

3. Seleccione la cantidad de accesos promedio o potenciales que se realizan en el transcurso de una jornada laboral estándar.

Menos de 10 accesos	
Menos de 20 accesos	

Menos de 30 accesos	
Menos de 40 accesos o más	

TERCERA PARTE Riesgo por tipo de entorno

4. Seleccione los entornos desde los cuales se acceden a los datos personales.

Físico (archivero de la unidad)	
Equipo de cómputo	
Nube (intranet, dropbox, google drive, etc.)	
Internet (portal de la SCJN)	

CUARTA PARTE Medidas de seguridad administrativas

5. Para la operación de las actividades del área a su cargo, ¿cuáles son las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional? (adjunte el documento que detalle dichas acciones).
6. Para la operación de las actividades del área a su cargo, ¿cuáles son las políticas y procedimientos para la identificación, clasificación y borrado seguro de la información y cómo se implementan? (adjunte el documento que detalle dichas acciones).

QUINTA PARTE Medidas de seguridad físicas

7. De las siguientes medidas de seguridad físicas, seleccione aquellas que son implementadas directamente por el área a su cargo:

Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información	
Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información	
Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización	
Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad	

8. En caso de haber seleccionado alguna opción anterior, detalle, por cada una de ellas, de qué manera es implementada (adjunte el documento que detalle dichas acciones).
9. En caso de contar con otro tipo de medidas de seguridad, detalle de qué manera son implementadas (adjunte el documento que detalle dichas acciones).

SEXTA PARTE Medidas de seguridad técnicas

10. De las siguientes medidas de seguridad técnicas, seleccione aquellas que son implementadas directamente por el área a su cargo:

Prevenir que 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 para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones	
Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware	
Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales	

11. En caso de haber seleccionado alguna opción anterior, detalle, por cada una de ellas, de qué manera es implementada (adjunte el documento que detalle dichas acciones).
12. En caso de contar con otro tipo de medidas de seguridad, detalle de qué manera son implementadas (adjunte el documento que detalle dichas acciones).

Suprema Corte de Justicia de la Nación

ANEXO 6. Nivel de riesgo latente por tratamiento

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
A1	Dirección General de Recursos Humanos.	Evaluación Psicométrica	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)	[redacted]				
A2	Dirección General de Recursos Humanos.	Servicio Social	DATOS ACADÉMICOS					
A3	Dirección General de Recursos Humanos.	Expedientes de Personal	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
A4	Dirección General de Recursos Humanos.	Fondo de Ahorro Capitalizable (FONAC)	DATOS SOBRE LA SALUD					
A5	Dirección General de Recursos Humanos.	Procesamiento de información para obtener cifras que se envían a terceros institucionales públicos y privados (juzgados familiares, ISSSTE, FOVISSSTE, bancos y beneficiarios particulares por disposición judicial).	DATOS SOBRE LA SALUD					
A6	Dirección General de Recursos Humanos.	Sistema de Ahorro para el Retiro (SAR).	DATOS IDENTIFICATIVOS					

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
A7	Dirección General de Recursos Humanos.	Elaboración de Contratos por Honorarios Asimilados a Salarios.	DATOS ACADÉMICOS	[redacted]				
A8	Dirección General de Recursos Humanos.	Becas - SCJN.	DATOS ACADÉMICOS					
A9	Dirección General de Recursos Humanos.	Capacitación.	DATOS ACADÉMICOS					
A10	Dirección General de Recursos Humanos.	Prácticas judiciales.	DATOS ACADÉMICOS					
A11	Dirección General de Recursos Humanos.	Trámite para el Apoyo y Ayuda de Anteojos.	DATOS SOBRE LA SALUD					
A12	Dirección General de Recursos Humanos.	Inscripción a Actividades Socioculturales y Deportivas para el personal de la SCJN.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
A13	Dirección General de Recursos Humanos.	Inscripción a Actividades Socioculturales y Recreativas para Jubilados y Pensionados del PJF.	DATOS SOBRE LA SALUD					
A14	Dirección General de Recursos Humanos.	Expediente Administrativo de los Infantes.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
A15	Dirección General de Recursos Humanos.	Expediente Administrativo de Apoyo Económico.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
A16	Dirección General de Recursos Humanos.	Movimientos Afiliatorios ante el ISSSTE.	DATOS LABORALES					

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
A17	Dirección General de Recursos Humanos.	Registro de datos personales en el Seguro de Separación Individualizado.	DATOS LABORALES	[redacted]				
A18	Dirección General de Recursos Humanos.	Registro de datos personales en el Seguro de Vida e Invalidez Total y Permanente.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
A19	Dirección General de Recursos Humanos.	Registro de datos personales en el Fondo de Reserva Individualizado.	DATOS LABORALES					
A20	Dirección General de Recursos Humanos.	Registro de datos personales en el Seguro de Gastos Médicos Mayores.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
B1	Dirección General de la Coordinación de Compilación y Sistematización de Tesis.	Suscripción a la Gaceta del Semanario Judicial de la Federación y venta de publicaciones.	DATOS ELECTRÓNICOS					
B2	Dirección General de la Coordinación de Compilación y Sistematización de Tesis.	Emisión de constancias por asistencia a curso de capacitación	DATOS ELECTRÓNICOS					
C1	Dirección General de Recursos Materiales.	Proveedores de bienes y servicios	DATOS PATRIMONIALES					
D1	Dirección General de Relaciones Institucionales.	Registro de asistentes a eventos organizados por la DGRI	DATOS ELECTRÓNICOS					

[redacted]

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
D2	Dirección General de Relaciones Institucionales.	Realizar invitaciones a eventos y envío de libros.	DATOS ELECTRÓNICOS	[redacted]				
D3	Dirección General de Relaciones Institucionales.	Registro de estancias de estudio y visitas oficiales al extranjero.	DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS					
E1	Dirección General de Comunicación Social.	Boletín Electrónico de la Suprema Corte.	DATOS ACADÉMICOS					
E2	Dirección General de Comunicación Social.	SIA	DATOS ELECTRÓNICOS					
E3	Dirección General de Comunicación Social.	#N/A	#N/A					
E4	Dirección General de Comunicación Social.	COFIDI.	DATOS ELECTRÓNICOS					
E5	Dirección General de Comunicación Social.	Directorio Nacional de Universidades e Instituciones de Educación Superior.	DATOS ELECTRÓNICOS					
E6	Dirección General de Comunicación Social.	Directorio de Medios de Comunicación.	DATOS ELECTRÓNICOS					
E7	Dirección General de Comunicación Social.	Directorio de la Dirección General.	DATOS ELECTRÓNICOS					
F1	Dirección General de Casas de la Cultura Jurídica.	Inscripción en la Plataforma Electrónica de Acompañamiento y Seguimiento para el Aprendizaje.	DATOS ACADÉMICOS					
				[redacted]				

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
F2	Dirección General de Casas de la Cultura Jurídica.	Registro Único de Disertantes.	DATOS ACADÉMICOS	[redacted]				
G1	Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos.	Protocolos de Actuación.	DATOS ELECTRÓNICOS					
G2	Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos.	Registro de participantes cursos virtuales "Acceso a la justicia especializada en niñez y adolescencia" y "Psicología forense en especializada en niñas, niños y adolescentes".	DATOS ELECTRÓNICOS					
G3	Dirección General de Estudios, Promoción y Desarrollo de los Derechos Humanos.	Registro de participantes a cursos y talleres presenciales.	DATOS ELECTRÓNICOS					
H1	Dirección General Tesorería.	Base de Viáticos.	DATOS IDENTIFICATIVOS					
H2	Dirección General Tesorería.	Relación de Pagos Electrónicos.	DATOS PATRIMONIALES					
I1	Secretaría de Seguimiento de Comités de Prestaciones Complementarias.	Tramitación de Solicitudes de Prestaciones Médicas Complementarias Programadas o por Emergencia Médica.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
				[redacted]				

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
I2	Secretaría de Seguimiento de Comités de Prestaciones Complementarias.	Trámite de pago de facturas por la adquisición de artículos promocionales de la SCJN.	DATOS ELECTRÓNICOS	[redacted]				
I3	Secretaría de Seguimiento de Comités de Prestaciones Complementarias.	Tramitación de Solicitudes de Pensiones Complementarias Mandos Superiores.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
I4	Secretaría de Seguimiento de Comités de Prestaciones Complementarias.	Tramitación de Solicitudes de Pensiones Complementarias Mando Medio y Personal Operativo.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
J1	Dirección General de Servicios Médicos.	Registro de Pacientes y Expediente Clínico Electrónico.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
K1	Centro de Estudios Constitucionales.	Registro de asistentes a eventos del Centro de Estudios Constitucionales.	DATOS ELECTRÓNICOS					
K2	Centro de Estudios Constitucionales.	Datos de ponentes de eventos para trámite de transportación y hospedaje.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
K3	Centro de Estudios Constitucionales.	Datos de autores para pago por elaboración de libros y artículos.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
				[redacted]				

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
K4	Centro de Estudios Constitucionales.	Datos de autores para la autorización de publicación de libros y artículos.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)	[redacted]				
K5	Centro de Estudios Constitucionales.	#N/A	#N/A					
K6	Centro de Estudios Constitucionales.	#N/A	#N/A					
L1	Centro de Documentación y Análisis, Archivos y Compilación de Leyes.	Atención a personas privadas de su libertad.	DATOS IDENTIFICATIVOS					
L2	Centro de Documentación y Análisis, Archivos y Compilación de Leyes.	Búsqueda y préstamo de expedientes judiciales.	DATOS IDENTIFICATIVOS					
L3	Centro de Documentación y Análisis, Archivos y Compilación de Leyes.	Control de acceso a inmuebles.	DATOS ELECTRÓNICOS					
L4	Centro de Documentación y Análisis, Archivos y Compilación de Leyes.	Servicio del sistema bibliotecario.	DATOS ELECTRÓNICOS					
L5	Centro de Documentación y Análisis, Archivos y Compilación de Leyes.	Servicio de consulta de acervo legislativo.	DATOS ELECTRÓNICOS					
M1	Comisión Substanciadora única del Poder Judicial de la Federación.	Acuerdos, notificaciones y resoluciones.	DATOS ESPECIALMENTE					

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
			PROTEGIDOS (SENSIBLES)	[redacted]				
N1	Dirección General de Presupuesto y Contabilidad.	Solicitud de Pagos.	DATOS SOBRE LA SALUD					
N2	Dirección General de Presupuesto y Contabilidad.	Catálogo de acreedores.	DATOS LABORALES					
N3	Dirección General de Presupuesto y Contabilidad.	Guarderías.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
N4	Dirección General de Presupuesto y Contabilidad.	Catálogo de firmas.	DATOS IDENTIFICATIVOS					
O1	Dirección General de Infraestructura Física.	Catálogo referencial de contratistas.	DATOS ACADÉMICOS					
P1	Dirección General de Seguridad.	Registro de entrada.	DATOS ELECTRÓNICOS					
P2	Dirección General de Seguridad.	Circuito cerrado de televisión.	DATOS BIOMÉTRICOS					
Q1	Unidad General de Transparencia y Sistematización de la información judicial.	Servicio social.	DATOS ACADÉMICOS					
Q2	Unidad General de Transparencia y Sistematización de la información judicial.	Resultados de evaluaciones psicométricas.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
				[redacted]				

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
Q3	Unidad General de Transparencia y Sistematización de la información judicial.	Formato de procedimiento sumario.	DATOS ACADÉMICOS	[redacted]				
Q4	Unidad General de Transparencia y Sistematización de la información judicial.	Formato de procedimiento ordinario.	DATOS ACADÉMICOS					
Q5	Unidad General de Transparencia y Sistematización de la información judicial.	Consulta física y electrónica de expedientes.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
Q6	Unidad General de Transparencia y Sistematización de la información judicial.	Formatos de procedimiento de acceso a la justicia.	DATOS ELECTRÓNICOS					
Q7	Unidad General de Transparencia y Sistematización de la información judicial.	Recibos de pago.	DATOS IDENTIFICATIVOS					
Q8	Unidad General de Transparencia y Sistematización de la información judicial.	Solicitudes de personas privadas de su libertad.	DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS					
Q9	Unidad General de Transparencia y Sistematización de la información judicial.	Atención ciudadana.	DATOS IDENTIFICATIVOS					

[redacted]

Clave del tratamiento	Área responsable	Tratamiento	Categoría de datos personales	Riesgo por tipo de dato	Accesibilidad	Anonimidad	Riesgo latente (máximo)	Nivel de riesgo
R1	Dirección General de Responsabilidades Administrativas y de Registro Patrimonial.	Recepción de declaraciones patrimoniales y de Intereses.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)	[redacted]				
R2	Dirección General de Responsabilidades Administrativas y de Registro Patrimonial.	Expediente de responsabilidades administrativas	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
R3	Dirección General de Responsabilidades Administrativas y de Registro Patrimonial.	Expediente de inconformidades	DATOS ACADÉMICOS					
R4	Dirección General de Responsabilidades Administrativas y de Registro Patrimonial.	Expediente de conciliaciones	DATOS ACADÉMICOS					
S1	Unidad General de Investigación de Responsabilidades Administrativas.	Procedimiento de Investigación de Responsabilidad Administrativa.	DATOS ESPECIALMENTE PROTEGIDOS (SENSIBLES)					
T1	Dirección General de Asuntos Jurídicos.	Tramitación de juicios, medios de defensa, responsabilidades administrativas, opiniones jurídicas y propiedad intelectual.	DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS					

ANEXO 7. Catálogo de medidas de seguridad para los tratamientos de datos personales

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; y, *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[5] 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

[5] 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

seguro de 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.[6]
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, 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.

[6] 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

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

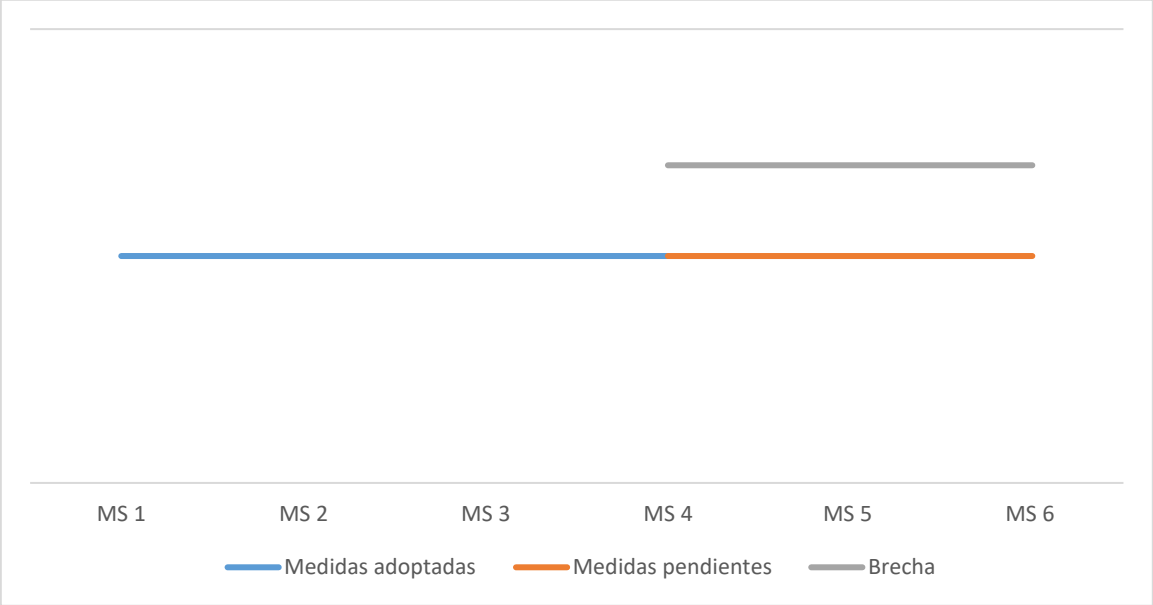
Es necesario recordar que estas medidas de seguridad son complementarias y refuerzan aquellas implementadas como política institucional de seguridad en la SCJN, coordinadas por las áreas competentes, entre ellas, la Dirección General de Seguridad y la Dirección General de Tecnologías de Información.

V. Análisis de brecha

El análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.

Por ejemplo, si se recomienda implementar al tratamiento "A" un conjunto de medidas "C", y el área responsable de dicho tratamiento informa que de ese conjunto de medidas hacen falta implementar algunas, la identificación de lo que hace falta implementar se conoce como brecha.

Análisis de brecha



El análisis de brecha es de naturaleza diagnóstica y contribuirá a conocer las áreas de oportunidad por cada tratamiento. A su vez, esta información dará sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar, en su momento, por el Comité de Transparencia para atenderlas de manera paulatina y en coordinación con cada una de las áreas.

ANEXO 8. Encuesta sobre análisis de brecha

Área**:**
Tratamiento
Nivel de riesgo:

RECOMENDACIÓN: Para contestar esta encuesta, se recomienda consultar los documentos "Catálogo de Medidas de Seguridad y Metodología" y la "Relación de los tratamientos de datos personales y el riesgo latente calculado".

13. De las siguientes medidas de seguridad administrativas, seleccione aquellas que ya son implementadas en el tratamiento de datos personales

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[7] 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 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.	

[7] 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

MEDIDAS DE SEGURIDAD — Físicas

14. De las siguientes medidas de seguridad físicas, seleccione aquellas que ya son implementadas en el tratamiento de datos personales:

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.[8]	
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, 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.	

[8] 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

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

15. De las siguientes medidas de seguridad técnicas, selecciones aquellas que ya son implementadas en el tratamiento de datos personales:

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.	

Suprema Corte de Justicia de la Nación

ANEXO 9. Análisis de brecha

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
A1	[redacted]																													
A2																														
A3																														
A4																														
A5																														
A6																														
A7																														
A8																														
A9																														
A10																														
A11																														

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
A12	[redacted]																													
A13																														
A14																														
A15																														
A16																														
A17																														
A18																														
A19																														
A20																														
B1																														
B2																														
C1																														
	[redacted]																													

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
D1	[redacted]																													
D2																														
D3																														
E1																														
E2																														
E3																														
E4																														
E5																														
E6																														
E7																														
F1																														
F2																														
G1																														

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
G2	[redacted]																													
G3																														
H1																														
H2																														
I1																														
I2																														
I3																														
I4																														
J1																														
K1																														
K2																														
	[redacted]																													

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
K3	[redacted]																													
K4																														
K5																														
K6																														
L1																														
L2																														
L3																														
L4																														
L5																														
M1																														
N1																														
N2																														
N3																														

[redacted]

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
N4	[redacted]																													
O1																														
P1																														
P2																														
Q1																														
Q2																														
Q3																														
Q4																														
Q5																														
Q6																														
Q7																														
Q8																														
Q9																														
	[redacted]																													

			Medidas de seguridad administrativas											Medidas de seguridad físicas							Medidas de seguridad técnicas						Brecha			
Clave	**Riesgo latente**	**Nivel de riesgo**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**A**	**B**	**C**	**D**	**E**	**F**	**Admva.**	**Física**	**Técnica**	**Total**
R1	[redacted]																													
R2																														
R3																														
R4																														
S1																														
T1																														
U1																														

[redacted]

PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

Fecha de clasificación	17 de febrero de 2020.
Área	Secretaría del Comité de Transparencia
Documento	Documento de Seguridad de la Suprema Corte de Justicia de la Nación
Tipo de clasificación	Reserva parcial respecto del análisis de niveles de riesgo y análisis de brecha
Fundamento legal	El artículo 113, fracciones I y VIII de la Ley General de Transparencia y Acceso a la Información Pública en relación con diverso 110, fracciones I y VII de la Ley Federal de Transparencia y Acceso a la Información Pública
Observaciones	Se suprime en **color negro** los resultados del análisis de niveles de riesgo y el análisis de brecha
Firma del titular	**Ariel Efrén Ortega Vázquez** **Secretario del Comité de Transparencia**