Suprema Corte de Justicia de la Nación

Informe final

en materia de protección de datos personales

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Unidad General de Transparencia y Sistematización de la Información Judicial

Versión final: diciembre 13 del 2022

Informe final UGTSIJ – datos personales

2019 – 2022

CONTENIDO

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Informe final UGTSIJ – datos personales

2019 – 2022

PRESENTACIÓN

En enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) 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 reconoció a la Suprema Corte de Justicia de la Nación (SCJN) como sujeto obligado para cumplir con los deberes reconocidos por dicha ley.

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

A partir del año 2019, por encargo del propio Comité de Transparencia, teniendo como base las actividades desplegadas durante 2018, la UGTSIJ emprendió una cadena de acciones y trabajos que implicaron análisis, diseño, sensibilización, capacitación, retroalimentación, evaluación, recopilación y sistematización de información, datos y medidas de seguridad institucionales, con la participación de todas las áreas que reportaron tratamientos de datos personales.

Sin una estructura definida en la UGTSIJ para atender las obligaciones en la materia, las actividades para dar cumplimiento a las disposiciones legales y reglamentarias se desarrollaron directamente por parte de la Dirección General, cuya coordinación se encargó al Mtro. Benjamín Alejandro Cervantes Pérez (Dictaminador II), con el apoyo eventual del Mtro. Gabriel Haquet Torres (Director), Lic. Gustavo Martínez Peña (Subdirector) y Andrés Landeros Bojorges (Técnico Operativo).

Este sexto y último informe semestral, se presenta al Comité de Transparencia como el INFORME FINAL en el que se hace un recuento de todas las acciones emprendidas y las medidas implementadas en la materia, para dejar evidencia, en un mismo documento, sobre el estado de cosas institucional en el cumplimiento de las obligaciones en materia de protección de datos personales, y ofrecer algunas reflexiones finales que contribuyan a transitar a una segunda etapa que, necesariamente, tendrá que confeccionarse a partir de enero de 2023, tomando como referencia el camino andado en estos años de trabajo.

Finalmente, este informe contiene los elementos necesarios para confeccionar un nuevo DOCUMENTO DE SEGURIDAD y con ello se detone una segunda etapa institucional en el rubro.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Informe final UGTSIJ – datos personales

2019 – 2022

RESUMEN EJECUTIVO

El INFORME FINAL realiza un recuento de las acciones más relevantes realizadas entre 2019, fecha en que se gestaron los primeros documentos que marcarían la ruta para la política institucional, y 2022, fecha que se estableció como límite para implementar el primer PLAN DE TRABAJO en materia de protección de datos personales de este Alto Tribunal.

El primer apartado se ocupa de la creación y aprobación del DOCUMENTO DE SEGURIDAD y del PLAN DE TRABAJO, sus propósitos y alcances como documentos que dan sustento a la política institucional en el rubro.

El segundo apartado se abordan los elementos que conforman el DOCUMENTO DE SEGURIDAD: inventario de tratamientos, avisos de privacidad, análisis de riesgos y análisis de brecha. Se realiza un recuento de la implementación de los insumos, los resultados más relevantes, sus actualizaciones y el estado de cosas que guardan a la fecha del presente informe.

El tercer apartado refiere al PORTAL DE DATOS PERSONALES como una acción fundamental para fortalecer la cultura de protección de datos personales en la institución, una herramienta que ayudó a consolidar las medidas de seguridad que se diseñaron e implementaron, y un insumo que se perfiló como el primer acercamiento a lo que debe ser un sistema de gestión.

El siguiente apartado se encarga de recapitular sobre las medidas administrativas, físicas y técnicas de seguridad que se planearon e implementaron conforme al PLAN DE TRABAJO, todas ellas reflejadas en insumos puestos a disposición en el PORTAL DE DATOS PERSONALES.

El quinto apartado se ocupa, brevemente, del tratamiento y gestión que se realizó para los datos personales relacionados con la emergencia sanitaria por Covid-19 desde la perspectiva de su confidencialidad y seguridad. En el sexto apartado se da cuenta de la implementación de los mecanismos de monitoreo y revisión, como una segunda etapa del PLAN DE TRABAJO, cuya finalidad fue reforzar el nivel de cumplimiento de las medidas de seguridad implementadas.

El apartado siete refiere a la Evaluación Diagnóstica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que se realizó en octubre de 2022 en materia de protección de datos personales y la habilitación de un espacio específico en el PORTAL DE DATOS PERSONALES donde se alojaron los formatos y criterios para dicha evaluación.

En el apartado ocho se aborda el diseño y desarrollo del Sistema de Gestión para la Protección de Datos Personales (SG-PDP) que se ha encaminado como un proyecto informático para la consolidación del cumplimiento legal de las obligaciones en la materia, al ser un medio que facilitará la autogestión, evaluación y monitoreo permanente y actualizado en la materia, cuyo proyecto obtuvo un premio a nivel nacional.

En el apartado final, se realizan una serie de reflexiones a la luz del recuento de estos tres años de trabajo, para visualizar un siguiente plan de trabajo, robustecerlo y dotarlo de una perspectiva renovada, tomando en consideración los cimientos que se han consolidado en la institución.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Documento de Seguridad y Plan de Trabajo

La Ley General 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 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. La Ley General 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

En ese sentido, a propuesta de la UGTSIJ, el 11 de septiembre de 2019, el Comité de Transparencia de la SCJN aprobó el Documento de Seguridad institucional en su décima sesión pública extraordinaria, el cual integró: i) inventario de tratamientos de datos personales, ii) análisis de riesgo, iii) catálogo de medidas de seguridad y iv) análisis de brecha.

Dicho documento y acta de aprobación pueden consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/documentos-relevantes/documento-seguridad

El propósito de que el Documento de Seguridad contuviera solo estos elementos fue presentar una primera radiografía institucional en materia de protección de los datos personales en su faceta administrativa, que reflejara las fortalezas, los pendientes y las áreas de oportunidad; y, constituyera un insumo para la toma de decisiones por parte de las instancias competentes en ese renglón para la implementación de acciones y medidas al respecto.

Con base en dichos hallazgos, en términos de los artículos 35 fracción V y 84 fracciones IV y V de la Ley General, el Comité de Transparencia instruyó a la propia UGTSIJ para que elaborara un plan de trabajo relacionado con el Documento de Seguridad.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Por ello, la UGTSIJ perfiló el PLAN DE TRABAJO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES (PLAN DE TRABAJO) como una herramienta complementaria y de instrumentalización del DOCUMENTO DE SEGURIDAD previamente aprobado por el Comité de Transparencia, cuyos objetivos fundamentales fueron los siguientes:

1. Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,
2. Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

El PLAN DE TRABAJO fue aprobado por el propio Comité de Transparencia el 12 de noviembre de 2019, cuyo documento y acta de aprobación pueden consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/documentos-relevantes/plan-trabajo-materia-proteccion-datos-personales.

Este documento contempló la implementación de medidas de seguridad administrativas, técnicas y físicas, entre las que se previó un listado de personal que interviene en tratamientos de datos personales; capacitación al personal responsable en la materia, y, mecanismos de monitoreo y revisión. Es decir, entre el DOCUMENTO DE SEGURIDAD y el PLAN DE TRABAJO, se contemplaron todos los elementos previstos en el artículo 35 de la Ley General, por lo que ambos constituyen la base de la política institucional en materia de protección de datos personales.

El PLAN DE TRABAJO se previó ejecutar en un periodo de tres años que, acorde al periodo de administración de la Presidencia del Ministro Arturo Zaldívar Lelo de Larrea (2019-2022), se implementó en dos etapas que se relacionaron con los propios objetivos: i) eliminar las brechas en las medidas de seguridad; e, ii) implementar mecanismos de monitoreo.

Por esa razón, en el segundo semestre de 2022, el DOCUMENTO DE SEGURIDAD debía actualizarse con la intención de entregar una radiografía actualizada en lo que respecta al inventario de tratamientos de datos personales, el análisis de riesgos y el análisis de brecha. Esto fue fundamental, por una parte, en tanto los tratamientos de datos personales se encuentran en constante evolución (creación, eliminación, fusión o actualización) y, por potra parte, porque se han implementado o sugerido todas las medidas de seguridad contempladas en el PLAN DE TRABAJO, lo que se reflejaría, cuando menos, en una brecha que se acerque al cien por 100% de cumplimiento.

Con la intención de profundizar en la explicación y detalle de cada una de las acciones emprendidas en el marco de estos documentos fundamentales, en el siguiente apartado se realiza un recuento de cada uno de los insumos que contempla el DOCUMENTOS DE SEGURIDAD para identificar el estado de cosas en que se encuentran.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

ELEMENTOS DEL DOCUMENTO DE SEGURIDAD: IMPLEMENTACIÓN Y ACTUALIZACIONES

1) Inventario de tratamientos

El INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES (INVENTARIO) es el control documentado que se lleva a cabo de los tratamientos de datos personales que realizan las áreas/órganos, realizado con orden y precisión, contemplado en los artículos 33, fracción III y 35, fracción I de la Ley General como un elemento del DOCUMENTO DE SEGURIDAD. La primera versión de dicho documento se realizó en el primer semestre de 2018, en el que la UGTSIJ trabajó con las áreas bajo la premisa de una coordinación interna para localizar todas las bases de datos personales de carácter administrativo 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 actualmente se identifican en el inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa
- Nombre del tratamiento
- Finalidad
- Fundamento normativo
- Datos personales que se recaban
- 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
- Referencia documental conforme al CADIDO vigente.
- Información sobre transferencias de datos personales
- Plazo de conservación

El INVENTARIO se actualiza permanentemente de conformidad con la información o los cambios que las propias áreas responsables solicitan a la UGTSIJ en cada uno de los elementos de los tratamientos de datos personales o, en su caso, por su registro inicial, fusión o eliminación. A partir de 2019, se publican semestralmente las versiones actualizadas del propio INVENTARIO a través de nuestro PORTAL DE DATOS PERSONALES.

Este insumo ha implicado retroalimentación y acompañamiento permanente para orientar y sensibilizar al personal involucrado con los tratamientos de datos personales sobre las obligaciones en la materia. La importancia de registrar la información exacta de los procesos que implican tratamiento de datos, además de cumplir con una obligación legal, radica en que las propias áreas puedan contar con esa información de manera permanente para ubicar e identificar los procesos que implican tratamiento de datos personales y el personal responsable de proteger, con un enfoque particular, el ciclo de vida de los datos personales que se tratan en las actividades cotidianas.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

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

En un principio se contó con el registró de 21 áreas y/u órganos que tratan datos personales, con un total de 80 tratamientos registrados. La última actualización de noviembre 2022 cuenta con 24 áreas y/u órganos administrativos de este Alto Tribunal, con un total de 98 tratamientos de datos personales. Esta versión se puede consultar en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/ITDP-10-octubre-2022.pdf

Cabe resaltar que el 29 de julio de 2020, el Presidente de la SCJN emitió el Acuerdo General de Administración II/2020 (AGA II/2020), con el propósito de establecer los lineamientos de seguridad sanitaria durante la emergencia generada por el virus SARS-CoV2 (COVID-19). Este acuerdo estableció, entre otras cosas, que los titulares de las áreas tenían la facultad de recabar datos personales de salud de su personal, particularmente sobre diagnósticos confirmados positivos de COVID-19 o síntomas asociados a dicha enfermedad, con el propósito de monitorear el estado de salud de las personas servidoras públicas, así como para la confección de las células de trabajo presenciales.

En ese sentido y por sus propias características, la materialización de estos deberes debía considerarse un tratamiento de datos personales sensibles, en términos de la ley. Derivado de lo anterior y como una medida preventiva, esta UGTSIJ elaboró las *Recomendaciones para los tratamientos de datos personales relacionados con la emergencia sanitaria por COVID-19*, que desarrollan una serie de medidas para que las áreas recaben y traten adecuadamente los datos relacionados con el estado de salud de las personas.

Estas Recomendaciones pueden consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/Recomendaciones-COVID-19%20Datos%20Personales.pdf

Como resultado, 24 áreas reportaron nuevos tratamientos relacionados con la emergencia sanitaria por el virus SARS-COV-2 (COVID-19) en el INVENTARIO. Dicho tratamiento aparece y se replica como responsabilidad de la mayoría de éstas, tiene carácter temporal y la información debe conservarse hasta en tanto finalice la emergencia sanitaria o se determine que la información cumplió con su finalidad, circunstancia que puede suceder en el transcurso del próximo año.

Asimismo, en abril de 2021, con la finalidad de identificar en cada uno de los tratamientos la clave archivística a la que se debía sujetar la temporalidad del tratamiento y conservación de sus documentos y archivos que lo componían, se solicitó al Centro de Documentación y Análisis, Archivos y Compilación de Leyes (CDAACL) el análisis del INVENTARIO para establecer esa información con base en el Catálogo de Disposición Documental (CADIDO) vigente.

A raíz de ese trabajo conjunto, se sugirió eliminar tratamientos (archivos y documentos) que debían considerarse de apoyo informativo en virtud de que no se relacionaban con las atribuciones de áreas y/u órganos, integrar o fusionar diversos tratamientos que correspondían a una misma serie por parte del área responsable; o separar tratamientos que se integraban como uno mismo.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

La importancia de este ejercicio fue materializar una adecuada conservación y depurado de documentos y archivos, físicos y electrónicos que contengan datos personales, las cuales son medidas de seguridad que se reconocieron en el PLAN DE TRABAJO y que más adelante se profundizan.

2) Avisos de Privacidad

El AVISO DE PRIVACIDAD (AVISO) tiene como finalidad contar con un instrumento que permita, por un lado, cumplir con el principio de informar a las personas titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales; y, por otro lado, que puedan tomar decisiones informadas respecto a dichos tratamientos (artículo 26).

De conformidad con la Ley General, el AVISO 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 (artículos 27 y 28).

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

La Ley General reconoce que el consentimiento puede otorgarse de manera tácita, cuando habiéndose puesto a disposición del titular el AVISO, éste no manifieste su voluntad en sentido contrario. Esto es así, ya que el AVISO 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 requiera la obtención del consentimiento expreso (artículo 21).

Para determinar qué tratamientos requerían –o no– AVISO, se partió de la premisa que la Ley General 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 Ley General, 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 una relación jurídica que pueda justificar el tratamiento.

Así lo perfiló el Comité de Transparencia el 22 de febrero de 2017 en su Cuarta Sesión Pública, en la que determinó, ante la consulta que realizó la Secretaría de Seguimiento de Comités de Prestaciones Complementarias, en torno a la Ley General, que no es necesario contar con el consentimiento previo de los titulares para su tratamiento, en tanto se actualiza un supuesto de excepción en términos de la fracción V del artículo 22; en consecuencia, no se desprende obligación de generar el aviso de privacidad.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

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 Ley General, necesitarían un AVISO. Esto resultó en su adopción y los modelos e información de cada caso fueron acordados con las propias áreas/órganos responsables de su implementación.

Los AVISOS simplificados fueron elaborados para que se colocaran en las instalaciones de cada una de las áreas responsables que así lo requirieran, en tanto se recaban datos de manera presencial; mientras que los integrales se ubicaron en el repositorio de avisos de privacidad integrales del PORTAL DE DATOS PERSONALES.

Los tratamientos que cuentan con AVISOS se pueden consultar en el reportorio: https://datos-personales.scjn.gob.mx/avisos-de-privacidad

Cabe señalar que los AVISOS se actualizan constantemente por parte de las áreas u órganos, en tanto se modifican los tratamientos de datos personales o se registran nuevos que lo requieren. La UGTSIJ funciona como facilitadora de la publicación de los AVISOS integrales; por tanto, la implementación del aviso simplificado, así como la actualización de los avisos integrales, corren a cargo de las áreas u órganos responsables.

3) Análisis de Riesgos

Para la confección del DOCUMENTO DE SEGURIDAD y ante la necesidad de determinar las medidas de seguridad que debían adoptar las áreas responsables, resultaba necesario conocer el nivel de riesgo que representaba cada tratamiento de datos personales (artículos 32, fracción I, 33, fracción IV y 35, fracción III de la Ley General). 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.

En el cálculo del nivel de riesgo de cada uno de los tratamientos registrados se usó la Metodología de Análisis de Riesgo BAA, la cual 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.

La metodología específica que se usó para el análisis de riesgo en este Alto Tribunal puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Metodolog%C3%ADa%20Riesgo%20y%20Brecha%202022.pdf

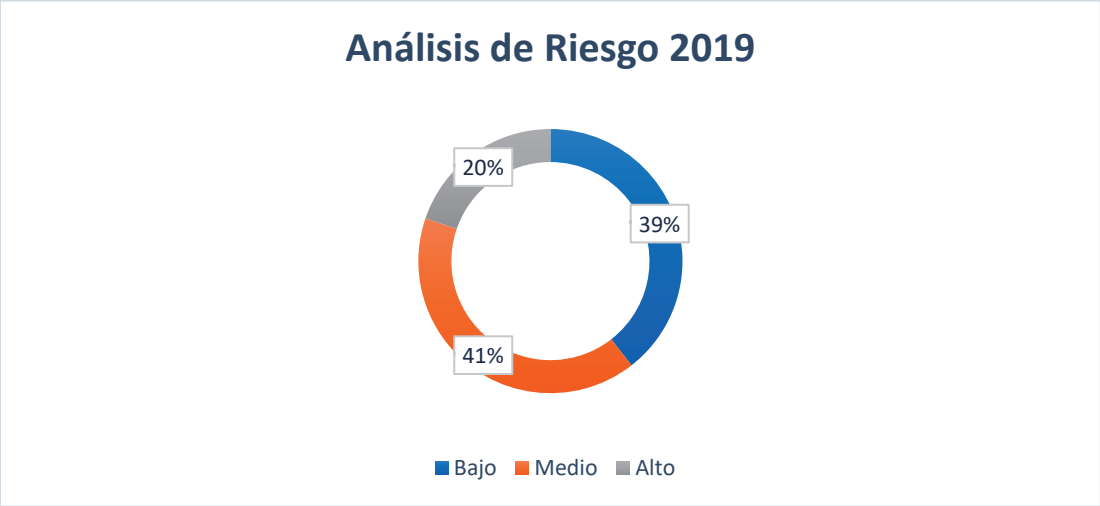
Con la finalidad de analizar datos objetivos, actuales y fidedignos para la elaboración del primer análisis de riesgo, se diseñó y aplicó en el año de 2019 la "Encuesta sobre análisis de riesgos y medidas de seguridad".

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 y se integraron al DOCUMENTO DE SEGURIDAD.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

A partir del PLAN DE TRABAJO, particularmente a las DIRECTRICES PARA LA IMPLEMENTACIÓN DE MECANISMOS DE MONITOREO Y REVISIÓN (DIRECTRICES), previstas para la segunda etapa de aquél, se contempló la actualización de este indicador como una de las acciones para la reformulación del DOCUMENTO DE SEGURIDAD.

El primer análisis de riesgos del año 2019 se realizó sobre 80 tratamientos de datos personales registrados en ese momento, de 21 áreas u órganos de carácter administrativo, cuya cantidad de tratamientos ilustrada en porcentajes por nivel riesgo fueron los siguientes:



Por su parte, la actualización de septiembre de 2022 se realizó sobre 97 tratamientos de datos personales registrados, de 23 áreas u órganos administrativos, cuya cantidad de tratamientos ilustrada en porcentajes por nivel de riesgo fueron los siguientes:

En 2022 la actualización de este indicador se realizó a través de la herramienta *Forms*, en la que las personas designadas como responsables de seguridad de cada área u órgano que tiene registrados tratamientos de datos personales respondieron la encuesta electrónica, misma que facilitó su llenado y el análisis de datos.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

El Reporte de Riesgo 2022 ilustra el nivel de riesgo de cada uno de los tratamientos por área u órgano, mismo que se acompaña al presente como **ANEXO 1,** y la base de datos completa que registra toda la información que se reportó conforme al formulario puesto a disposición, se acompaña como **ANEXO 2.**

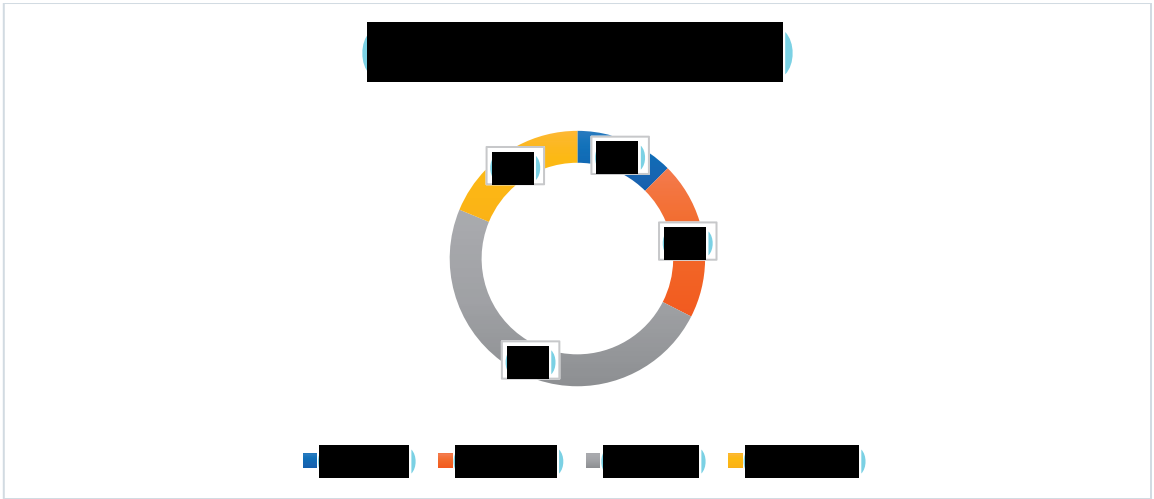
4) Análisis de Brecha

El análisis de brecha permite identificar la distancia que existe entre las medidas recomendadas, en el CATÁLOGO DE MEDIDAS DE SEGURIDAD (CATÁLOGO), y las medidas implementadas por cada uno de los tratamientos reportados. Por ejemplo, si se recomienda implementar al tratamiento un conjunto de medidas y el área responsable informa que hacen falta implementar algunas, la identificación de lo que hace falta se conoce como brecha.

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

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 y puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Catalogo-Medidas-Seguridad-SCJN.pdf

En el mes de mayo de 2019 y teniendo como referencia el CATÁLOGO, se elaboró la primera "Encuesta sobre análisis de brecha", 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 las implementadas y las que aún estaban pendientes de ello. [redacted]



KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Posteriormente, a partir de la implementación del PLAN DE TRABAJO, particularmente las DIRECTRICES previstas para la segunda etapa de aquél, se contempló la actualización de este indicador como una de las acciones para reformular el DOCUMENTO DE SEGURIDAD. Igual que el indicador anterior, el trabajo del nuevo análisis de brecha se realizó de manera electrónica a través de la aplicación *Forms*.

[redacted]

Una vez que se obtuvieron los niveles de brecha de los tratamientos registrados por las áreas y los órganos conforme a las respuestas que fueron registradas por las personas responsables y la aplicación de la metodología diseñada para ello, se compartió el Comparativo de Brecha 2019-2022 de cada uno de sus tratamientos, con la advertencia de que algunos tratamientos no contaban con dicho comparativo en tanto no se tenían registrados en el primer ejercicio o, en su caso, fueron tratamientos que desaparecieron.

El Comparativo de Brecha 2019-2022 de todos los tratamientos que permite visualizar el grado de cumplimiento de las medidas de seguridad recomendadas, después de la implementación del PLAN DE TRABAJO en la materia, se acompaña a este informe como **ANEXO 3,** y la base de datos completa que registra toda la información que se reportó por las áreas y órganos en el análisis de brecha conforme al formulario puesto a disposición, se acompaña como **ANEXO 4.**

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

PORTAL DE PROTECCIÓN DE DATOS PERSONALES

La habilitación del PORTAL DE DATOS PERSONALES, en donde se alojan los insumos y documentos que soportan la política institucional en el rubro, fue fundamental para consolidar una cultura de protección de datos personales al interior de este Alto Tribunal y facilitar la puesta a disposición del material que refleja el cumplimiento de las obligaciones legales. Es un espacio para rendir cuentas a las personas titulares de los datos y al organismo garante sobre el tratamiento de los datos personales, y poner a disposición de las personas que integran este Alto Tribunal la información necesaria para consolidar la política institucional en el rubro.

Su formación comenzó desde el PLAN DE TRABAJO donde se estimó viable la modernización de los procesos en los tratamientos de datos personales que permitiera, por ejemplo, la utilización de herramientas software adecuadas y la automatización en las fases que integran los mencionados procesos.

Por su parte el INAI, a través del *Acuerdo mediante el cual se aprueba la adición de un título décimo de los lineamientos generales de protección de datos personales para el sector público*, ordenó a los sujetos obligados habilitar en su portal de internet un apartado denominado "Protección de datos personales", el cual debía contar, cuando menos, con los avisos de privacidad e información relevante en materia de protección de datos personales. Dicho apartado serviría para rendir cuentas del cumplimiento de las obligaciones en el rubro, tanto a las personas titulares, como al propio instituto referido.

Bajo esta coyuntura y como iniciativa de la UGTSIJ se gestó, en coordinación con la DGTI, el espacio en el portal institucional destinado a la protección de datos personales. Este proyecto fue más ambicioso que la obligación referida en el Acuerdo del párrafo que antecede, pues pretendía ser el cigoto del eventual SG – PDP.

La estructura actual de contenidos del PORTAL se compone de los siguientes elementos: Avisos de Privacidad, Derechos ARCO, Capacitación, Documentos Relevantes, Medidas de Seguridad, Normativa en la Materia, Evaluación INAI y Contacto, Dudas o Quejas.

La propuesta del PORTAL DE DATOS PERSONALES fue puesta a consideración del Comité de Transparencia el 14 de abril de 2021. El 09 de junio de 2021 se aprobó el portal por dicho órgano colegiado y se liberó al público el día 5 de julio del mismo año por parte de la DGTI a través del enlace para su consulta.

Posteriormente, el 30 de septiembre del 2021, el INAI comunicó a los sujetos obligados una circular en la que recomendó que este apartado debía encontrarse en la página de inicio y al mismo nivel que la sección Transparencia, como un apartado independiente y exclusivo para la garantía del derecho a la protección de datos personales.

En ese sentido, se solicitó a la DGTI migrar la ubicación del portal del banner inferior, al banner superior, al mismo nivel que el de Transparencia en el portal principal de la SCJN. El enlace de consulta del portal es el siguiente: https://datos-personales.scjn.gob.mx/

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

MEDIDAS DE SEGURIDAD IMPLEMENTADAS CONFORME AL PLAN DE TRABAJO

Como se citó en el apartado que refiere al PLAN DE TRABAJO, este documento previó dos etapas que se relacionaron con sus propios objetivos: i) eliminar las brechas a través de la implementación de las medidas de seguridad; e, ii) implementar mecanismos de monitoreo.

Sobre la primera etapa, su propósito fundamental fue eliminar las brechas en los tratamientos de datos personales identificados en la SCJN, de manera que los recursos se encaminaron para que las medidas de seguridad recomendadas fueran implementadas o, en su caso, se encontraran en vías de implementación dentro del periodo en que se desarrolló.

Para esta etapa se tomó como referencia el CATÁLOGO, en donde se describen las medidas de seguridad administrativas, físicas y técnicas (artículo 31 de la Ley General). La meta que se fijó para esta primera etapa fue que todos los tratamientos de datos personales tuvieran un cumplimiento cercano al 100% de las medidas de seguridad recomendadas.

La meta que arrojó el último análisis de brecha fue de 96%, contando aquellos tratamientos de datos personales que se fueron incorporando en el transcurso de la implementación del propio PLAN DE TRABAJO.

A continuación, se desarrolla el estatus de cada una de las medidas de seguridad implementadas, identificándolas por su tipo.

1) Medidas de seguridad administrativas

- **Responsable de seguridad**

Esta medida de seguridad fue pilar para la implementación de todas las demás. El objetivo que se planteó para esta figura es que cada área u órgano que tratara datos personales designara una persona responsable de seguridad de datos personales para coordinar y auxiliar en la implementación de las medidas de seguridad establecidas, con el fin de que se preserven y exista una comunicación directa con la UGTSIJ.

Esta designación ocurrió en el primer trimestre del año 2020 por parte de las áreas y los órganos, a los que se les recomendó que la persona designada estuviera familiarizada con el tema de datos personales en su área y, en su caso, podría ser la misma que fungía como enlace de transparencia ante la UGTSIJ o que hubiese estado a cargo del tema en los meses recientes, lo cual dependería de los esquemas de organización de cada área, así como la cantidad y tipos de tratamientos.

En esa tesitura, se conformó el *Directorio de responsables de seguridad de datos personales de la SCJN*, con un registro actual de 24 personas a cargo del tema en las áreas administrativas que cuentan con tratamientos de datos personales. Cabe resaltar que son las áreas las que nombran o sustituyen a las personas responsables.

Este directorio se acompaña al presente informe como **ANEXO 5.**

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

- **Listado de personal que interviene en el tratamiento de datos personales**

La primera medida de seguridad que se implementó en todas las áreas de manera general fue de carácter administrativo y se trató del LISTADO DEL PERSONAL QUE INTERVIENE EN EL TRATAMIENTO DE DATOS PERSONALES (LISTADO) conforme al artículo 35, fracción II de la Ley General.

A principios de 2020, la UGTSIJ recapituló con todas las áreas sobre la aprobación del DOCUMENTO DE SEGURIDAD y del PLAN DE TRABAJO por parte del Comité de Transparencia en el año 2019, en donde se había perfilado que, a lo largo de todo el año 2020, se materializaría una parte del referido plan, cuyo propósito inicial era la implementación de las medidas de seguridad recomendadas.

En ese sentido, como primera medida, se les solicitó a todas las áreas que implementaran y resguardaran el LISTADO y remitieran a la UGTSIJ una copia, para formar parte de las medidas de seguridad contempladas en el PLAN DE TRABAJO. Se aclaró que debía elaborarse un listado por cada uno de los tratamientos registrados en el INVENTARIO.

Para facilitar la implementación de dicha medida, la UGTSIJ proporcionó los formatos de los listados correspondientes por cada uno de los tratamientos, los cuales permitieron identificar el área de que se trata, el tratamiento respectivo, el número de personas que intervienen en él, su nombre, su cargo, la dirección de su oficina, la función que realiza sobre el tratamiento, el formato en que lo realiza y el fundamento normativo que lo faculta para realizarlo.

Como producto de esta medida, se integró el LISTADO que permite identificar el universo de personas servidoras públicas que intervienen en los tratamientos de datos personales y dimensionar la importancia de regular dicha actividad en la SCJN.

Posteriormente, como un mecanismo de monitoreo y revisión, se solicitó a las áreas la actualización de esta medida de seguridad cada semestre. Estas actualizaciones se realizaron a través de la herramienta *SharePoint* en la que fue posible que las áreas registraran los cambios directamente en el archivo, sin necesidad de descargar o remitir documentación de prueba.

La última actualización ocurrió en octubre de 2022 y puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Listado-de-Personal-SCJN-Oct22.pdf

- **Declaratoria de confidencialidad**

La finalidad de esta medida de seguridad es que todas las personas que intervienen en los tratamientos de datos personales y se encuentren registradas en el LISTADO estén debidamente informadas de los deberes que les corresponden en términos de las disposiciones establecidas en la Ley General.

En ese sentido, la implementación se realizó en el primer trimestre de 2020 y se solicitó a las áreas/órganos que pusieran a disposición la DECLARATORIA DE CONFIDENCIALIDAD (DECLARATORIA) para su firma electrónica o autógrafa de las personas involucradas, resguardaran la evidencia y comunicaran a la UGTSIJ sobre la realización de dichas acciones.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

El formato de la DECLARATORIA se pone a disposición a través del siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Declaratoria-de-confidencialidad-lenguaje-incluyente.pdf

Como una herramienta complementaria de esta medida de seguridad, se elaboró la *Guía Básica para las personas que intervienen en el tratamiento de datos personales*, que permite a los responsables del tratamiento profundizar en los conceptos clave, los principios para el tratamiento de datos y las medidas de seguridad correspondientes. Esta Guía puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Declaratoria-de-confidencialidad-lenguaje-incluyente.pdf

Posteriormente y también como un mecanismo de monitoreo y revisión, se solicitó a las áreas/órganos que dispusieran de la actualización de la DECLARATORIA para el personal que no las hubiera signado debido a la actualización del LISTADO antes referido.

- **Clasificación y depurado de archivos físicos y electrónicos**

El DOCUMENTO DE SEGURIDAD y el PLAN DE TRABAJO contemplaron un par de medidas de seguridad administrativas: i) clasificación de los archivos físicos y electrónicos que contengan documentos vinculados con tratamientos de datos personales; y, ii) depurado y borrado seguro de los datos personales en términos de las disposiciones de la Ley General y los plazos de conservación en materia archivística (artículos 23 y 24 de la Ley General).

Bajo estas premisas, el CDAACL y la UGTSIJ trabajaron para que los tratamientos registrados en el INVENTARIO respondieran a la clasificación archivística dispuesta por los instrumentos aprobados por el propio CDAACL, así como al periodo de conservación y procedimientos de depuración, vinculándolo con el CADIDO.

De esta manera, además de la revisión y edición del INVENTARIO como se refirió en el apartado correspondiente, en la coyuntura de la confección y presentación del Acuerdo General de Administración XI/2021, relativo a la organización, conservación, administración y preservación de los archivos administrativos de este Alto Tribunal, la UGTSIJ colaboró con el CDAACL para que las disposiciones contenidas en dicho proyecto incluyeran una perspectiva de protección de datos personales, especialmente en la identificación de expedientes que contengan datos personales, supresión de dichos expedientes previo bloqueo, entre otras.

En esa tesitura, la UGTSIJ elaboró una propuesta de *Guía para la conservación y depuración de archivos que contiene datos personales* que fue puesta a consideración del CDAACL para conciliarla y difundirla entre las áreas con el propósito de identificar, sintetizar y sistematizar los elementos sustantivos para la conservación y depuración de archivos físicos y electrónicos, particularmente aquellos que contengan datos personales.

En noviembre de 2021 se difundió entre las áreas dicho insumo a través de una circular conjunta, en la que se señaló la obligación de este Alto Tribunal de observar la normativa archivística para la baja documental que resulte en la eliminación, borrado o destrucción de los datos personales (artículo 3, fracción XXX), así como la supresión de éstos cuando hayan dejado de ser necesarios

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

para el cumplimiento de las finalidades (artículo 23) y de establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales (artículo 24), en términos de la legislación general de la materia.

La Guía referida puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Gu%C3%ADa_conservaci%C3%B3n_eliminaci%C3%B3n_dp_v290921.pdf

- **Capacitación**

También como una medida administrativa, se incorporó en el PLAN DE TRABAJO una oferta de capacitación especializada al personal involucrado en el tratamiento de los datos personales. Por lo anterior, se incorporó un rubro en la materia en los Programas Anuales de Capacitación 2020, 2021 y 2022 aprobados por el Comité de Transparencia.

En ese sentido y bajo las premisas institucionales encaminadas a proteger la salud, propiciar un entorno seguro que redujera los riesgos asociados a la enfermedad COVID – 19 y previniera su transmisión ante la contingencia sanitaria, fue necesario ajustar las estrategias para el cumplimiento de las líneas de acción de los programas de capacitación, motivo por el cual se gestionaron licencias del software *Prezi*, que ayudó a construir contenidos digitales especializados en la materia y a potenciar el alcance de la capacitación, así como la gestión de talleres virtuales de capacitación a través de la plataforma *Teams*.

A lo largo de estos años, se diseñaron y elaboraron seis cápsulas informativas en torno a las generalidades de la protección de datos personales, las cuales se titulan como sigue: Recepción de datos personales, Conceptos clave, Principios, Avisos de privacidad, Documento de Seguridad y Portal de Dato Personales.

El universo de capacitación ha sido las personas designadas como responsables de seguridad, aquellas que recaban datos personales de primera mano por virtud de sus funciones, tales como recepcionistas, personal médico y de enfermería, organizadoras de eventos, entre otros, así como las personas que tratan datos personales al interior de este Alto Tribunal.

De esta manera, a través de las personas designadas como responsables, se ha solicitado que dicho personal consulte los contenidos de las cápsulas informativas para homologar los conocimientos generales en materia de datos personales y, al mismo tiempo, consolidar una cultura institucional de su debida protección.

Las cápsulas de capacitación están publicadas para su consulta permanente, en el siguiente apartado del Portal de Datos Personales: https://datos-personales.scjn.gob.mx/capacitacion

Por lo que toca a los talleres especializados, en 2021 se ofrecieron dos talleres a las personas designadas como responsables de seguridad, en conjunto con la DGTI:

– "Seguridad informática", ofrecido por el personal de la Dirección de Seguridad Informática de la DGTI el día 14 de mayo de 2021.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

- "Uso y cuidado de bienes informáticos", ofrecido por el personal de la Dirección de Cómputo Personal de la DGTI el día 31 de mayo de 2021.

Ambos talleres se desarrollaron de manera virtual a través de la herramienta *Teams*, en los que acudieron 47 y 44 personas servidoras públicas, respectivamente.

Por último, el 25 de febrero de 2022 se realizó un taller sobre conservación y eliminación de archivos que contengan datos personales, con la colaboración del CDAACL. Este taller estuvo dirigido a todas las personas responsables de seguridad en datos personales designadas por las áreas u órganos de su adscripción. Además de las 23 personas responsables asistentes, acudieron 33 interesadas en los temas y se tuvo una participación total de 56 personas.

- **Bitácora de vulneraciones**

El PLAN DE TRABAJO contempló implementar una BITÁCORA DE VULNERACIONES como medida de seguridad de carácter administrativo, cuyo propósito fue que cada área cuente con un control informativo en donde se reporten las vulneraciones de datos personales.

Por vulneraciones se deben entender, por lo menos, las siguientes circunstancias respecto de datos personales (en particular), bases de datos y/o sistemas que los albergan (en general): la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado; o, el daño, la alteración o modificación no autorizada.

Cuando se presenta alguna de estas situaciones, existe la obligación de analizar las causas por las cuales se presentó una vulneración e implementar acciones preventivas y correctivas para evitar que la vulneración afecte a más titulares y/o se repita (artículo 37 de la Ley General).

Además, si la vulneración tiene el riesgo de repercutir significativamente en los derechos patrimoniales o morales de sus titulares (por ejemplo, las sucedidas sobre datos sensibles), se debe informar sobre ésta, sin dilación alguna, a los titulares afectados y, según sea el caso, al organismo garante. Este aviso previene a los titulares para que puedan tomar las medidas correspondientes en la defensa de sus derechos (artículo 40 de la Ley General).

Para garantizar la atención adecuada de cualquier vulneración de datos personales, resultaba necesario que cada área de la SCJN contara con su propia BITÁCORA DE VULNERACIONES. Por ello, en agosto de 2020, la UGTSIJ puso a disposición de las áreas el *Instructivo para registrar y reportar vulneraciones de datos personales*, con la finalidad de que identifiquen y registren, adecuadamente, las vulneraciones ocurridas a la seguridad de los datos personales en sus actividades cotidianas.

En dicho documento se anexó un modelo de bitácora para que fuera adoptado por las áreas y, además de seguir el procedimiento desarrollado en el instructivo, se tuviera un registro homologado de cualquiera de las vulneraciones descritas en el artículo 37 de la Ley General.

El instructivo se encuentra disponible en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Instructivo-para-registrar-y-reportar-vulneraciones-de-Datos-Personales.pdf

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

- **Bitácora de consulta**

El PLAN DE TRABAJO contempló la implementación de la BITÁCORA DE CONSULTA como una medida de seguridad de carácter administrativa dirigida a los tratamientos con riesgo alto.

Derivado de la consulta realizada a la información registrada en el INVENTARIO y el análisis de riesgo del DOCUMENTO DE SEGURIDAD, se identificaron los tratamientos de las áreas de este Alto Tribunal cuyo nivel de riesgo es alto y que, además, contienen datos personales sensibles, ya que ambos elementos fueron considerados finalmente para recomendar la implementación de una BITÁCORA DE CONSULTA.

Además, teniendo en cuenta la prevalencia del esquema de trabajo a distancia derivado de la contingencia sanitaria, se recomendó implementar la BITÁCORA DE CONSULTA en aquellos tratamientos que se albergan en sistemas informáticos puestos a disposición por la DGTI o por un prestador de servicios externo. Posteriormente, se recomendó que, cuando fuera materialmente factible, se replicara esta medida para aquellos tratamientos que se albergan en archivo físico, en su caso.

La confección e implementación de esta medida de seguridad fue concertada en conjunto con la DGTI bajo las siguientes premisas:

- Una premisa conceptual a partir de la cual deberán considerarse los estándares de la BITÁCORA DE CONSULTA establecidos en el PLAN DE TRABAJO, así como aquellos que corresponden a las bitácoras que ya se encontraban implementadas en otros sistemas informáticos de este Alto Tribunal, las cuales contemplaban, al menos, lo siguiente: i) número consecutivo, ii) nombre del servidor público; iii) edificio y/o ubicación desde donde se accede; iv) fecha y horario de acceso; v) motivo de acceso al sistema: registro, consulta, modificación, edición, borrado, otro.
- Otra premisa operativa en virtud de la cual las áreas/órganos debían solicitar a la propia DGTI la implementación de la BITÁCORA DE CONSULTA (bajo los estándares citados) en los tratamientos de datos que correspondan.

Al momento de la presentación de este informe, se tiene lo siguiente:

Área	Tratamiento	Estatus
DGS	Circuito Cerrado de Televisión	Resuelta
	Sistema de Citas	Implementada
DGRH	Expediente de Personal	Solicitada
	Evaluación Psicométrica	Plataforma externa
	Nómina	Solicitada
	Ayuda de anteojos	Solicitada
DGSM	Expediente Médico	Implementada
DGRARP	Recepción de declaraciones patrimoniales y de intereses	Implementada (rubros pendientes)
	Expedientes de responsabilidades administrativas	Implementada
DGPC	Solicitud de Pagos (SIA)	Solicitada
UGIRA	Responsabilidades Administrativas	Implementada

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

- **Transferencias seguras**

En el PLAN DE TRABAJO se integró una medida de seguridad administrativa sobre transferencias de datos personales, cuya recomendación general es que éstas se realicen con las medidas de confidencialidad necesarias.

Derivado del análisis sobre la pertinencia de algunos tratamientos y del intercambio suscitado en reuniones con algunas áreas, se advirtió la necesidad de esta medida en tanto las transmisiones de datos personales fuera y dentro de la institución son una práctica cotidiana que presentaba diversas áreas de oportunidad para asegurar su confidencialidad.

En abril de 2020 se construyó la *Guía para la transmisión segura de datos personales*, en conjunto con la DGTI. Esta guía se perfiló desde la perspectiva de los principios que rigen en materia de protección de datos personales y se establecen en la Ley General.

En particular, el principio de proporcionalidad que mandata que los responsables del tratamiento de datos personales solo deberán tratar aquellos que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento (artículo 25 de la Ley General). Así como al principio de lealtad, que implica la obligación de este Alto Tribunal de privilegiar, en todo momento, el interés por el cual los titulares de los datos personales proporcionan su información y la expectativa razonable de privacidad en el tratamiento de sus datos (artículo 19 de la Ley General).

Se aclaró que las transmisiones de datos personales son toda comunicación de datos fuera del área responsable de su tratamiento, ya sea que éstas se hagan a otras áreas u órganos de la SCJN o incluso, a otras instituciones (transferencias).

Por ello, a través de comunicaciones enviadas en el mes de mayo de 2020, se sugirió a las áreas y los órganos analizar la pertinencia de compartir la información personal relacionada con los tratamientos registrados bajo su responsabilidad y, en caso de resultar necesario, considerar la adopción de las medidas de seguridad que se recomendaban en la Guía referida. La Guía está disponible en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Guia-para-la-transmision-de-datos.pdf

- **Clausulado para contratos con terceros encargados**

Esta medida de seguridad administrativa no se contempló de inicio en el PLAN DE TRABAJO; sin embargo, los hallazgos en el INVENTARIO y el análisis de la Ley General impulsaron a la UGTSIJ a proponer y poner a disposición un prototipo de clausulado en materia de protección de datos personales para los contratos que celebra la SCJN y actualizan la figura de los terceros encargados.

Esta propuesta tomó como referencia que la SCJN, como responsable de diversos tratamientos, está obligada a velar por la protección de los datos personales en su posesión o en posesión de un tercero ajeno a la institución que realice tratamientos a nombre y por cuenta de la SCJN.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

La Ley General define la figura del encargado como 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 (Artículo 3, fracción XV). Para definir el esquema de responsabilidades de este tipo de relaciones jurídicas, la propia ley dedica el Título Cuarto para desarrollar las obligaciones entre el responsable y el encargado.

A partir de la conformación del DOCUMENTO DE SEGURIDAD y la actualización permanente del INVENTARIO, se encontraron algunos en los que intervienen personas jurídicas ajenas a la institución (encargados) y que, más allá del acuerdo de confidencialidad, en los contratos que documentan esa relación jurídica no se incorporaba un clausulado enfocado a la protección especializada en datos personales, conforme a los parámetros de la Ley General.

La contratación de servicios de terceros relacionados con algunos tratamientos registrados implica el manejo de datos personales (registro, transferencia, resguardo, clasificación, entre otros), de manera que resultaba importante generar certeza y delimitar la responsabilidad para proteger a la SCJN del mal manejo o uso indebido que pudiera presentarse por parte de los encargados, sin menoscabo de que los contratos que no se vinculen con tratamientos a nombre y por cuenta de la SCJN, también delimitaran las responsabilidades en torno a los datos personales.

Por lo anterior, en el mes de febrero de 2021, en conjunto y a propuesta de la Dirección General de Asunto Jurídicos (DGAJ), se diseñó y compartió con las áreas cuyas atribuciones tienen a cargo la formalización de contrataciones (Recursos Materiales, Casas de la Cultura Jurídica e Infraestructura Física) el prototipo referido y se les solicitó considerar su implementación en los contratos suscritos por este Alto Tribunal que así correspondieran.

Dicho prototipo se encuentra disponible en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Prototipo-Clausulado-Proteccion-Datos-Personales-para-Contratos-SCJN-3ros-Encargados.pdf

2) Medidas de seguridad técnicas

El PLAN DE TRABAJO contempló una serie de medidas de seguridad físicas (cuidado de bienes informáticos) y técnicas (cuidado y actualización de la contraseña personal, respaldos frecuentes e instalación de softwares), que debían concretarse a través de materiales didácticos, mecanismos de difusión masiva y ajustes normativos.

Debido a que las medidas técnicas que se contemplaron en el PLAN DE TRABAJO podían agruparse en un solo insumo didáctico que abarcara todas, la UGTSIJ y la DGTI, elaboraron y difundieron la *Guía de seguridad informática para la protección de los datos personales*, cuyos propósitos fundamentales fueron:

- Fomentar una serie de medidas de seguridad para la protección de los bienes informáticos que almacenan datos personales y que se plasmaron en el PLAN DE TRABAJO; y
- Reforzar los alcances del Programa de Concientización y Capacitación en Seguridad Informática 2020 a cargo de la DGTI.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

El documento integra las siguientes recomendaciones y medidas de seguridad en materia informática para que las personas servidoras públicas de la SCJN se protejan de cualquier actividad maliciosa que ponga en peligro los bienes informáticos, la información que ahí se almacena y, en especial, los datos personales que se tratan en dichos bienes de conformidad con sus atribuciones y las disposiciones en la materia:

- Cuidado de los bienes informáticos (hardware).
- Instalación de dispositivos y software no autorizados.
- Traslado seguro de equipos de cómputo.
- Cuidado de las contraseñas.
- Respaldo de información.
- Uso del correo electrónico.
- Reporte de incidentes y vulneración de datos personales.

La *Guía de seguridad informática para la protección de los datos personales* puede consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Guia-seguridad-inform%C3%A1tica.pdf

3) Medidas de seguridad físicas

El PLAN DE TRABAJO contempló algunas medidas de seguridad físicas encaminadas a la prevención de accesos no autorizados a los archivos y/o equipos que contengan datos personales, particularmente las siguientes: i) archiveros, cajoneras y gavetas con candado/chapa; ii) candados de seguridad para equipos de cómputo; y, iii) zonas de confidencialidad, éstas últimas solo para aquellos tratamientos de datos personales con riesgo alto.

La implementación de estas medidas de seguridad se postergó debido a la crisis sanitaria por el virus SARS-COV-2 y a los esquemas de trabajo a distancia que se implementaron en este Alto Tribunal. Sin embargo, ante la incorporación paulatina del trabajo presencial, se realizaron las primeras gestiones en torno a estas medidas de seguridad.

- **Archiveros, cajoneras y gavetas con candado/chapa; y candados de seguridad para equipos de cómputo.**

En junio de 2022 se solicitó a las áreas y los órganos que realizan tratamientos de datos personales emprender las acciones conducentes para asegurar o, en su caso, reforzar las siguientes medidas de seguridad:

- Que los documentos -con independencia de su soporte documental- en los que figuren datos personales en términos del inventario de tratamientos institucional, sean resguardados en archiveros, cajoneras y/o gavetas utilizando los candados y/o chapas correspondientes.
- Que los equipos de cómputo que albergan documentos -con independencia de su soporte documental- o bases de datos en los que figuren datos personales en términos del inventario de tratamientos institucional, sean asegurados con candados de seguridad.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Sobre la implementación de esta medida se informó al Comité de Transparencia en el mes de agosto de 2022 a través del Quinto Informe Semestral, en el que se detalla la información que reportó cada una de las áreas/órganos: https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/Quinto-Informe-Semestral-CT.pdf.

- **Zonas de confidencialidad**

El PLAN DE TRABAJO también contempló la implementación de zonas de confidencialidad para el resguardo de documentos físicos vinculados con tratamientos de datos personales que se encuentran en la categoría de riesgo alto, en términos del análisis de riesgos previamente realizado.

Las zonas de confidencialidad se definen como los espacios para resguardar de manera segura los archivos físicos que contengan datos personales vinculados con tratamientos que se encuentran dentro de la categoría de riesgo alto, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado, a través de dispositivos de control como puertas con cerradura, tarjetas inteligentes o biométricos.

Como una primera gestión para la implementación de esta medida física de seguridad se emprendió un levantamiento de información que constituyera el insumo inicial para configurar un dictamen que, en conjunto con las áreas competentes, permitiera atender las particularidades de cada espacio físico y los volúmenes documentales.

Por lo anterior, el pasado 14 de junio de 2022 se solicitó a las áreas que realizan tratamientos de datos personales con riesgo alto que proporcionaran dicha información preliminar y reportaron sustancialmente lo siguiente:

- No requiere zona de confidencialidad por ser tratamiento electrónico:
  - Dirección General de Servicios Médicos
- Sí cuentan con zonas de confidencialidad:
  - Dirección General de Recursos Humanos.
  - Dirección General de Presupuesto y Contabilidad.
- Requieren adecuaciones de los espacios:
  - Dirección General de Responsabilidades Administrativas y de Registro Patrimonial.
  - Dirección General de Seguridad.
  - Unidad General de Investigación de Responsabilidades Administrativas.

Con esa información preliminar, el pasado 14 de octubre de 2022 se solicitó el apoyo a la Dirección General de Infraestructura Física (DGIF), con miras a confeccionar un dictamen que determine las necesidades y acciones que deban realizarse para implementar zonas de confidencialidad.

Bajo esa tesitura, se realizó una reunión presencial entre las personas que operarían dichas acciones de ambas direcciones y, posterior a dicha reunión, se realizaron las primeras visitas de inspección a la DGRARP y a la UGIRA. Esto permitirá elaborar un primer dictamen que contenga, entre otras cosas, las necesidades y requerimientos para materializar zonas de confidencialidad, así como la ruta crítica para implementarlas.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Se tiene pendiente la atención a la DGS, en tanto se debe atender la ordenación y depuración de su archivo físico en todos los edificios de este Alto Tribunal para determinar la pertinencia de una zona de confidencialidad para esos archivos. También se tiene pendiente la atención a aquellas áreas que sí cuentan con zonas de confidencialidad con el propósito de reforzar y/o validar su seguridad.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

MECANISMOS DE MONITOREO Y REVISIÓN

La segunda etapa del PLAN DE TRABAJO, calendarizada para realizarse en 18 meses (agosto 2021-diciembre 2022), tuvo como objetivo fundamental preservar el nivel de cumplimiento y protección conseguido en la primera etapa a través de la implementación de mecanismos de monitoreo y revisión de las medidas de seguridad, además de la mejora de los procesos en el tratamiento de los datos personales y el acompañamiento para la ejecución de todas las medidas de seguridad.

Por lo anterior, se formularon las mencionadas DIRECTRICES como un primer acercamiento que orientara el diseño y la implementación de los mecanismos para fortalecer el cumplimiento de las medidas de seguridad en los tratamientos de datos personales (contemplando su nivel de riesgo), a partir de los cuales fuera posible integrar a todas las áreas que tratan datos personales, generar un diálogo sobre el estado de cosas y detonar acciones en función del resultado de los monitoreos.

Las DIRECTRICES pueden consultarse en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Directrices-Implementacion-Mecanismos-Monitoreo-y-Revision_2.pdf

En ellas se consideraron que los mecanismos de monitoreo y revisión debían tener estos propósitos:

- Actualizar los insumos y las medidas de seguridad que así lo requieran.
- Reforzar las recomendaciones que se realizaron a través de las medidas de seguridad implementadas en la primera etapa del PLAN DE TRABAJO.
- Establecer un espacio de trabajo en el que se resuelvan dudas e inquietudes sobre el tema, se identifiquen posibles amenazas o vulneraciones y se robustezca la cultura de la protección de datos personales en la institución.

La implementación de los mecanismos se realizó a través de aplicaciones de *Office 365*, utilizando el PORTAL DE DATOS PERSONALES y el correo electrónico institucional para aplicar y difundir las herramientas creadas entre cada una de las áreas involucradas en el tratamiento de datos personales. Estas herramientas ayudaron a recopilar y sistematizar la información y facilitar la identificación de estrategias para reforzar las medidas de seguridad, de acuerdo con las necesidades de cada área.

1) Actualización de indicadores y medidas de seguridad

Por su naturaleza, algunos indicadores y/o medidas de seguridad debían actualizarse periódicamente para mantenerlas vigentes y actualizadas. Como un mecanismo de monitoreo y revisión, se calendarizó la actualización semestral del LISTADO y de la DECLARATORIA, tal como se explicó en los apartados correspondientes a estas medidas de seguridad.

Por otra parte, en virtud de que se debía actualizar el DOCUMENTO DE SEGURIDAD a la luz de la implementación de las medidas de seguridad previstas en el PLAN DE TRABAJO, se actualizaron el inventario de tratamientos (semestralmente), el análisis de riesgo y el análisis de brecha, con los resultados antes descritos.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

2) Cuestionarios de Monitoreo

Los cuestionarios de monitoreo tuvieron como propósito evaluar el nivel de conocimiento e involucramiento del personal de este Alto Tribunal que interviene en el tratamiento de datos personales en torno a los conceptos y temas en la materia. Tuvieron el carácter de voluntarios, por tanto, las respuestas que se registraron fueron anónimas.

- **Primer cuestionario de monitoreo**

El 29 de septiembre de 2021, la UGTSIJ difundió el *Primer Cuestionario de Monitoreo* a través de la aplicación *Forms*, dirigido a las personas designadas como responsables en materia de datos personales, con la finalidad de recoger sus impresiones a partir de sus experiencias suscitadas en los últimos meses y, con ello, identificar áreas de oportunidad en la materia, así como los rubros temáticos que constituyeron la agenda del Grupo de Trabajo integrado por las propias personas responsables de seguridad y el personal especializado de la UGTSIJ.

Las respuestas arrojaron, en términos generales, los siguientes hallazgos:

- La figura del responsable de seguridad ha impactado de forma positiva al interior de las áreas.
- Las personas que intervienen en los tratamientos de datos personales están regularmente familiarizadas con las recomendaciones y medidas de seguridad que se han divulgado.
- Las recomendaciones para permear el conocimiento de protección de datos personales en todas las personas involucradas son, entre otras, generar más capacitación y un programa de divulgación permanente y masivo.
- Es suficiente el acompañamiento y asesoría brindados por la UGTSIJ.
- Para la creación de un Grupo de Trabajo permanente, se consideró oportuno revisar temas como tratamientos de datos personales en la nube, uso de herramientas tecnológicas para archivos electrónicos y depuración de archivos que contienen datos personales.

El resumen de los resultados puede consultarse en el siguiente enlace: https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=IXFudvg3gBFRDmvgltn7Dtx22UF5UZMu&id=AewGDKrlVE6IEbuZhwsMd2zxvwWyGpdJgOduaaZppeBUOEhNNVQwWlM5T1dLVVFXMk9STTlWTjJTUy4u

- **Segundo cuestionario de monitoreo**

En el mes de marzo de 2022 se puso a disposición el *Segundo Cuestionario de monitoreo en materia de protección de datos personales*, esta vez dirigido a todas las personas que intervienen en el tratamiento de datos personales, cuyo propósito fue monitorear su nivel de involucramiento en los conceptos básicos. Participaron 598 personas y los resultados más relevantes fueron los siguientes:

Pregunta/planteamiento	Porcentaje de respuestas correctas
¿Qué debemos entender por derecho a la protección de datos personales?	98%
¿Qué son los datos personales?	84%

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Pregunta/planteamiento	Porcentaje de respuestas correctas
¿Qué son los datos personales sensibles?	98%
Definición de tratamiento de datos personales	88%
Característica de una fuente de acceso público	81%
¿Quién asume la figura de responsable en materia de protección de datos personales?	78%
¿Cómo se define la figura de encargado en el tratamiento de datos personales?	85%
¿Quién es el titular de los datos personales?	85%
Son principios que deben observarse en el tratamiento de datos personales	80%
¿Qué órgano aprobó el Documento de Seguridad y el Plan de Trabajo en la Suprema Corte de Justicia de la Nación?	77%

Para consultar el resumen de todas las respuestas, puede realizarse en el siguiente enlace: https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=jNMjpn9evpKMdD6LJsmGROFgbPAjDZSK&id=AewGDKrlVE6IEbuZhwsMd-YY3BCuKsVPq7swCTMsHLFUNUJFWVooNoVGUjhaSEdROFVNNTlYMDgyMy4u

- **Tercer cuestionario de monitoreo**

Posteriormente, en el mes de junio de 2022 se puso a disposición el *Tercer Cuestionario de monitoreo en materia de protección de datos personales* dirigido a las personas que intervienen en los tratamientos de datos personales, cuyo propósito fue monitorear el nivel de involucramiento en el tema de la transmisión segura de datos personales. En esta ocasión participaron 636 personas y los resultados más relevantes son los siguientes:

Pregunta/planteamiento	Porcentaje de respuestas correctas
De acuerdo con la Guía para la transmisión segura de datos personales, ¿una transmisión de datos es?	95%
El principio de proporcionalidad mandata que los responsables deben tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.	76%
El principio de lealtad ordena privilegiar en todo momento la protección del interés del titular por el que otorgó sus datos personales y su expectativa razonable de privacidad.	74%
Definición de transferencia de datos personales.	91%
Estándares de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para las transferencias de datos personales.	84%
Ejemplos de transmisiones físicas de datos personales las siguientes.	67%
Medida de seguridad más recomendable para la transmisión segura de datos personales en forma física.	86%
Información confidencial a través de correo electrónico es un ejemplo de transmisión electrónica.	98%
Encriptar o cifrar archivos es un procedimiento que impide que la información electrónica sea visible y servible para las personas no autorizados a conocerla:	90%

El resumen de los resultados puede consultarse en el siguiente enlace: https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=YZDQl69WcR3pZ3YHleVgWyAL9rLCu2VF&id=AewGDKrlVE6IEbuZhwsMd-YY3BCuKsVPq7swCTMsHLFUQlMzOEdRUFUzUU5QMVg5VUxKSlNFNEtQQi4u

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

- **Cuarto cuestionario de monitoreo**

Finalmente, en el mes de noviembre de 2022 se puso a disposición el *Cuarto Cuestionario de monitoreo en materia de protección de datos personales*, cuyo propósito fue monitorear el nivel de involucramiento en el tema de vulneración de datos personales y seguridad informática. En esta ocasión participaron 817 personas y los resultados más relevantes son los siguientes:

Pregunta/planteamiento	Porcentaje de respuestas correctas
Tipos de vulneraciones de seguridad de datos personales.	95%
Persona a quien se debe informar en primera instancia una vulneración, de conformidad con el *Instructivo para registrar y reportar vulneraciones de datos personales*.	86%
La bitácora de vulneraciones es el documento que garantiza una atención adecuada a las vulneraciones de datos personales y que debe quedar bajo resguardo del área u órgano responsable.	90%
Caso donde se debe informar a las personas titulares de los datos personales y al organismo garante sobre una vulneración de datos personales.	75%
Es uno de los propósitos de la Guía de seguridad informática para la protección de los datos personales.	96%
Medidas básicas que contempla la *Guía de seguridad informática para la protección de los datos personales* para hacer buen uso de los bienes informáticos y proteger la información que ahí se almacena.	96%
¿Qué son los bienes informáticos, descritos en la *Guía de seguridad informática para la protección de los datos personales*?	94%
Recomendación relacionada con abstenerse de instalar dispositivos o software no autorizado.	91%
Medida para el cuidado correcto de la contraseña personal.	88%
Qué se debe hacer en caso de un incidente o posible evento que constituya un riesgo sobre bienes o servicios tecnológicos.	95%

El resumen de los resultados puede consultarse en el siguiente enlace: https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=gwtDtAAKJxMjFZ5FWUpompNGtaJ9mXNn&id=AewGDKrlVE6IEbuZhwsMd-YY3BCuKsVPq7swCTMsHLFUM05VNlE4NDFNVjkyRVhESVoySlVJN101Ni4u

3) Grupo de Trabajo

Como parte de los mecanismos de monitoreo, se creó un GRUPO DE TRABAJO entre la UGTSIJ y los responsables de seguridad de datos personales a través de la aplicación *Yammer*, como un espacio institucional destinado para compartir reflexiones, dudas o sugerencias en torno a la protección de datos personales.

Tiene el carácter de permanente y voluntario, sirve para identificar áreas de oportunidad en la implementación de la política institucional en materia de datos personales, a partir de las experiencias de los responsables de seguridad, las dificultades que ha representado este ejercicio y los temas que decidan poner a consideración y se encuentra disponible en: https://web.yammer.com/main/groups/eyJfdHlwZSI6Ikdyb3VwIiwiaWQiOiI3NzU2OTQ1ODE3NiJ9/all

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Para formalizar el GRUPO DE TRABAJO, compartir experiencias en la protección de los datos personales y presentar los resultados del Primer Cuestionario de Monitoreo, se celebró una primera reunión de trabajo virtual a través de la herramienta *Teams* con los responsables de seguridad el 19 de octubre de 2021, a la cual asistieron 24 personas.

Asimismo, en el contexto de la actualización del Análisis de Brecha 2022, en el mes de septiembre del 2022 se convocó a una reunión a través del GRUPO DE TRABAJO con los responsables de seguridad de cada una de las áreas, para resolver dudas, aclarar la metodología de la actualización y presentar el formulario que se puso a disposición con la finalidad de contar con resultados más certeros.

4) Campaña de difusión institucional – Infografías

Como un mecanismo de monitoreo y revisión se planeó el reforzamiento de conocimiento y de medidas de seguridad a través de infografías periódicas. El objetivo de las infografías ha sido reforzar la cultura de la protección de datos personales.

Esta actividad se realiza en colaboración con la Dirección General de Comunicación Social (DGCS), a través de la cuenta institucional "La Corte informa" que tiene alcance a todo el personal de este Alto Tribunal; además, las infografías se encuentran publicadas para su consulta permanente en el banner de inicio del Portal de Datos Personales https://datos-personales.scjn.gob.mx/.

Las infografías difundidas hasta el momento son las siguientes:

Mes	Tema	Enlace de consulta
Enero	Principios y conceptos clave	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-05/01-Datos-Personales.pdf
Febrero	Tratamiento de datos personales	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-05/tratamiento%20de%20datos%20%281%29.pdf
Marzo	Responsabilidad en el tratamiento de datos personales.	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-05/datos_p_v2_0.pdf
Abril	Transmisión segura de datos personales.	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-06/04-Infografia-Transmision-Datos-Personales.pdf
Mayo	Avisos de privacidad.	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-06/05-Infografia-Avisos-Privacidad.pdf
Junio	Vulneración de datos personales.	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-07/06-Infografia-Vulneracion-Seguridad-Datos-Personales.pdf
Agosto	Tratamiento de datos personales por terceros encargados	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-09/07-Infografia-Terceros-Encargados.pdf
Septiembre	Conservación y eliminación de datos personales	https://datos-personales.scjn.gob.mx/sites/default/files/carrusel-principal/archivos/2022-11/Infografia%20Conservacion%20y%20Eliminacion%20Datos%20Personales.png_.pdf
Noviembre	Política institucional en datos personales	https://intranet.scjn.pjf.gob.mx/PDF/Banner_principal/politica-de-datos-personales.pdf

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

EVALUACIÓN INAI

El 17 de noviembre de 2021 el INAI aprobó el Acuerdo ACT-PUB/17/11/2021.05, mediante el cual se aprueban los *Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del desempeño de los sujetos obligados del sector público federal en cumplimiento a la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados.*

De conformidad con estos instrumentos técnicos, la evaluación para los sujetos obligados mediría y analizaría 6 vertientes, 9 variables, 10 formatos y 41 criterios; cuyo cumplimiento sería evaluado a partir del número de criterios cumplidos por responsable.

Las vertientes hacen referencia a los principios, deberes y obligaciones con los que deben cumplir los sujetos obligados a partir de lo establecido en la Ley General y demás disposiciones aplicables en la materia. Por su parte, las variables refieren a diversos aspectos de los principios, deberes u obligaciones identificados en cada una de las vertientes y de ellas se derivan los criterios incluidos en los formatos. A su vez, los criterios se refieren a cada dato o rubro de información que los responsables deben organizar, actualizar, validar y remitir, dentro de los formatos que se publican en el apartado virtual "Protección de Datos Personales".

Formatos e indicadores para evaluación de desempeño de la SCJN		
Vertiente		Formato
1	Principios	1.1 Aviso de privacidad integral.
		1.2 Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General.
2	Deberes	2.1 Deber de seguridad.
		2.2 Deber de confidencialidad y comunicaciones de datos personales.
3	Ejercicio de los derechos ARCO	3.1 Mecanismos para el ejercicio de los derechos ARCO.
4	Portabilidad	4.1 Portabilidad de datos personales.
5	Evaluación de impacto en la protección de datos personales	5.1 Evaluación de impacto en la protección de datos personales
6	Responsables en materia de protección de datos personales	6.1 El Comité de Transparencia y la Unidad de Transparencia. 6.2 Oficial de Protección de Datos Personales.

El medio a través del cual se dispuso a realizar la evaluación fue el PORTAL DE DATOS PERSONALES, lo que permitió al INAI evaluar el cumplimiento de los principios, deberes y obligaciones en la materia de manera virtual. Para facilitar esa evaluación, se habilitó un apartado especial en el portal titulado *Evaluación INAI*, donde se alberga la información necesaria en los formatos que fueron objeto de evaluación por parte del organismo garante: https://datos-personales.scjn.gob.mx/evaluacion-inai

Con el propósito de verificar que la información puesta a disposición en el apartado del PORTAL DE DATOS PERSONALES cumpliera con los formatos y criterios establecidos por el órgano garante, el 01 de septiembre de 2022 esta UGTSIJ solicitó una asesoría técnica para la implementación de los instrumentos técnicos de evaluación emitidos por el INAI.

Una vez que se tuvo conocimiento de las observaciones y comentarios sobre los formatos y criterios, el 07 de octubre de 2022 se sostuvo una reunión virtual entre las personas responsables por parte de la UGTSIJ y de la Dirección General de Evaluación, Investigación y Verificación del

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Sector Público del INAI, para concordar los últimos detalles en la información publicada en ese repositorio.

De conformidad con el Programa de Evaluación Anual 2022-2023 del INAI, se realizaría una única evaluación de tipo diagnóstico en la que se podría emitir recomendaciones de carácter general respecto de los hallazgos de la evaluación. Se tuvo previsto que, en la primera fase implementada en el mes de octubre de 2022, se evaluaría al Poder Judicial de la Federación.

De conformidad con el Programa referido, el INAI tiene previsto notificar y publicar los resultados de la evaluación en el mes de abril de 2023.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Sistema de Gestión

Desde la publicación de la Ley General, la implementación de cada una de las disposiciones y obligaciones legales ha significado un reto para este Alto Tribunal y, particularmente, para las personas involucradas en el tema, en la medida que representó procesos y conceptos novedosos al interior. Además, se ha enfrentado a la falta de interpretación oportuna y homogénea sobre los alcances de dichas disposiciones, con la complejidad que ello significa en la materialización de insumos, indicadores, informes y/o cumplimientos de los principios y deberes.

Por ejemplo, para la confección de uno de los primeros insumos en la materia, relativo al Inventario de Tratamientos de Datos Personales que debía recabarse al interior de la SCJN, se sugirió, por parte del órgano garante, el uso de un archivo Excel que permitiera recabar una serie de información sobre los procesos y actividades de cada una de las áreas/órganos que representaran tratamientos de datos personales. Por ello, para solicitar esta información, orientar a las personas responsables sobre su llenado, recabarla, limpiarla y sistematizarla, debían transcurrir varias semanas con el propósito de contar con un insumo más o menos acabado.

Esto se replicaba para cada indicador o insumo que debía implementarse, de conformidad con los principios y deberes, tales como avisos de privacidad, listado de personas que intervienen en los tratamientos y sus funciones, análisis de riesgos, análisis de brecha, documento de seguridad, etcétera.

Por otro lado, destaca la disposición legal que refiere a que las acciones relacionadas con las medidas de seguridad para el tratamiento de datos personales deberán estar documentadas y contenidas en un sistema de gestión. La Ley General, en su artículo 34, refiere como sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales (artículo 34, Ley General). Es decir, es el nodo que debe contener todo lo referente a la política institucional en el rubro.

En una primera instancia, el Portal de Datos Personales se gestó como el cigoto de un sistema de gestión que permitiera convertirse en un espacio de consulta permanente para titulares de datos personales, personas servidoras públicas involucradas en el tema y público en general. Sin embargo, no resultaba suficiente para automatizar procesos y autogestión de medidas de seguridad.

Bajo este contexto, la UGTSIJ diseñó un sistema informático para materializar un SG – PDP que permita a las áreas/órganos emprender acciones y consultar insumos en materia de protección de datos personales en un solo espacio digital, autogestionar la implementación, operación, actualización, monitoreo y revisión de los principios y las medidas de seguridad de los tratamientos bajo su responsabilidad.

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

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

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

A la fecha del presente informe, se compartió con la DGTI la primera fase de desarrollo del SG-PDP, acompañado de la documentación necesaria que explica la funcionalidad, alcance y beneficios a la institución de la implementación de un sistema de esta envergadura, con la expectativa de que la intervención de esa área técnica coadyuvará a la culminación de las últimas etapas del desarrollo, así como su instalación y puesta en marcha.

El resultado esperado es que el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, se puedan realizar desde un mismo sitio y que ahí mismo se alojen todas las referencias documentales que la institución deba elaborar y poner a disposición de su personal.

Este proyecto refleja varios años de trabajo y definiciones en la implementación de las obligaciones y disposiciones legales en la materia, lo cual supondrá dos beneficios concretos del SG – PDP:

- La síntesis y minimización de los procesos internos para la implementación y cumplimiento de cada uno de los principios y deberes previstos en la Ley General, lo que redundará en ahorro de tiempo y de recursos (humanos y materiales).
- La UGTSIJ y el Comité de Transparencia podrán verificar, a través de un solo sitio digital, el nivel de cumplimiento y la atención a los requerimientos en la materia en tiempo real. Asimismo, las personas responsables de las áreas y los órganos que tratan datos personales podrán verificar, consultar y actualizar la información en torno a los tratamientos bajo su responsabilidad.

Todo lo anterior trascenderá efectivamente en el nivel de protección de los datos personales, el nivel de cumplimiento en la materia y el ahorro de tiempo en las gestiones administrativas con esos propósitos.

Además, el proyecto del SG – PDP fue presentado el pasado 14 de octubre al certamen "Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales 2022" convocado, entre otras instituciones, por el INAI, siendo parte de un proyecto integral en conjunto con el Consejo de la Judicatura Federal.

Como resultado, el pasado 8 de diciembre del 2022, el Jurado del Premio otorgó el primer lugar a la postulación denominada: "Política de Innovación para la Protección de Datos Personales del Poder Judicial de la Federación (SCJN – CJF)", uno de cuyos componentes fue precisamente el SG – PDP. En el siguiente enlace se alberga la información respectiva: Ganadores (inai.org.mx).

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

REFLEXIONES FINALES

A tres años de implementación del PLAN DE TRABAJO y cuatro que comenzaron a interpretarse y materializarse las obligaciones legales en la materia, es posible concluir que los objetivos planteados al inicio de esta primera etapa se han cumplido.

Lo anterior obedece a que se implementaron las medidas de seguridad previstas y los mecanismos de monitoreo y revisión diseñados, se tiene un índice de brecha cercano al 100% de cumplimiento, se cuenta con una radiografía completa de todos los tratamientos de datos personales, se ha iniciado una cultura generalizada de protección de datos personales en todas las áreas u órganos de este Alto Tribunal a los que se dirigieron estos trabajos y se encuentran actualizados los inventarios, así como los análisis de riesgo y brecha para el siguiente documento de seguridad.

No obstante, se considera importante mencionar las áreas de oportunidad y enseñanzas que deja esta primera etapa, para integrarlas en un nuevo plan de trabajo de lo que debe ser la segunda etapa en esta materia.

Cabe resaltar que la primera de ellas, relacionada con el fortalecimiento de la estructura de la UGTSIJ para atender estos temas, necesariamente facilitaría y fortalecería las demás.

1) Área especializada y encargada del seguimiento de las políticas y procedimientos de protección de datos personales

Salvo el desahogo de solicitudes en materia de acceso, rectificación, cancelación y oposición de datos personales (ARCO), en 2015 la UGTSIJ no fue concebida orgánicamente para hacerse cargo de cuestiones en materia de datos personales pues tampoco existía una ley en ese renglón.

Posteriormente, como parte de la reforma al Reglamento Orgánico publicada el 20 de abril de 2022, se formalizaron las atribuciones de la UGTSIJ en materia de protección de datos personales que se refieren a:

- Administrar el portal de datos personales.
- Implementar y mantener los mecanismos y sistemas electrónicos para cumplir con las políticas y obligaciones en la materia.
- Recibir y gestionar las solicitudes ARCO, así como los medios de defensa que se interpongan en su caso.
- Analizar y proponer procedimientos internos para hacer más eficiente la gestión de solicitudes ARCO.
- Asesorar a los órganos y áreas en los tratamientos de datos personales.
- Fungir como enlace ante el órgano garante nacional.
- Proponer planes de capacitación.

Concluida la primera etapa en la materia y dadas las circunstancias en las que deberá diseñarse y aplicarse un nuevo plan de trabajo, se estima que ello implica responsabilidades relevantes de instrumentación, control y verificación de las obligaciones en el rubro.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=

Por ello, una propuesta viable es que dichas actividades sean responsabilidad de la actual Subdirección General de Transparencia y Acceso a la Información (SGTAI) y supervisadas/ejecutadas por una Dirección de Área.

En este contexto, se propone la creación de una dirección de área y de una jefatura de departamento a la cual se le adscribirían, a su vez, dos plazas operativas para hacer eficiente la operación con una visión de alcance transversal a todas las áreas administrativas y, en su caso, a los órganos de apoyo jurisdiccional. Con esta incorporación, la SGTAI tendría 3 direcciones a su cargo y sería necesaria la reorganización de las funciones de gestión de solicitudes de personas privadas de su libertad y de servicios al público.

El personal que se designe para atender estas tareas se abocará a la atención cotidiana de las áreas u órganos, capacitación constante y masiva, revisión de la implementación de las medidas de seguridad y coordinarán el diseño e implementación de la segunda etapa.

2) Estrategia de comunicación con las áreas responsables

La designación de una persona responsable por área u órgano coadyuvó a la gestión de requerimientos, implementaciones y actualizaciones. La intención de esta primera etapa se cumplió, en la medida que la comunicación planeada funcionó para que las áreas u órganos respondieran oportunamente.

No obstante, desde una perspectiva más exigente, este esquema no resulta eficiente en el momento en que se busca masificar y profundizar el conocimiento en todas las personas que intervienen en los tratamientos de datos personales. Factores como que las personas responsables cumplen varias funciones al interior de su área y el tema de protección de datos personales no se atendía de manera exclusiva, obstaculizarían este nivel de profundidad.

Por tanto, se debe planear una nueva estrategia de comunicación con las áreas responsables para permear en toda la institución y fortalecer el nivel de conocimiento en todas las personas servidoras públicas. Algunas sugerencias son:

- Designar una persona responsable por cada tratamiento de datos personales.
- Fortalecer el GRUPO DE TRABAJO y convertirlo en una red activa y propositiva en el tema.
- Abrir mecanismos de comunicación por parte de la UGTSIJ de fácil acceso (correo electrónico, chat, etc.) disponible a todo el personal para que resuelvan dudas de manera puntual y rápida.

3) Capacitación especializada y masiva

La capacitación debe retomarse en la segunda etapa en la materia con una perspectiva más robusta. La capacitación que se ofreció en la primera etapa, principalmente, estuvo dirigida a las personas designadas como responsables, cuya premisa ha sido la difusión del conocimiento al interior de sus áreas, además de la puesta a disposición de todos los materiales de capacitación e información en el PORTAL DE DATOS PERSONALES para su consulta permanente.

KkLwPJN/fuYpyci3ltj348uQjcpIPcf2J0jTI+8Vlek=

Sin embargo, cada tratamiento de datos personales representa retos diferentes para la confidencialidad de la información. Por ello, las personas que tratan cotidianamente los datos personales deben tener presente las recomendaciones en la materia y se hace necesaria una nueva planificación de capacitación que sea masiva, especializada para cada área u órgano, que se refleje en insumos específicos para atender problemáticas puntuales, que evalúe el nivel de conocimiento y que aproveche las herramientas tecnológicas.

4) Auditorías con perspectiva de datos personales

Los procesos que lleva a cabo la Dirección General de Auditoría podrían contar con una perspectiva de protección de datos personales para verificar el cumplimiento puntual de las obligaciones en la materia en cada área u órgano.

Para ello, es importante una colaboración conjunta entre la UGTSIJ y aquella dirección, con el propósito de dotar de esta perspectiva los procesos de auditoría, advirtiendo sobre las particularidades que presenta cada tratamiento de datos personales.

Además de ese procedimiento, un mecanismo de revisión y control mucho más robusto y constante es necesario para evaluar el cumplimiento. Que la UGTSIJ, a través del área que se encargue de este tema, tenga mayor presencia en la vigilancia de las actividades que implican tratamientos de datos personales, para resolver dudas, posibles vulneraciones, riesgos, debilidades en los procesos, siempre desde una perspectiva de respeto, responsabilidad y buena fe.

KkLwPJN/fuYpyci3ltj348uQjcplPcf2J0jTI+8Vlek=