



Suprema Corte
de Justicia de la Nación

Segundo informe semestral

Implementación del Plan de Trabajo en materia de
protección de datos personales

Unidad General de Transparencia y
Sistematización de la Información Judicial

Versión final: enero 18 del 2021

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

1. Presentación.

En términos del Documento de Seguridad aprobado por el Comité de Transparencia el 11 de septiembre de 2019 y del Plan de Trabajo en materia de protección de datos personales (PLAN DE TRABAJO), autorizado por dicho órgano colegiado el 12 de noviembre de 2019, la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTSIJ) presenta su **SEGUNDO INFORME SEMESTRAL** sobre la implementación de las medidas y acciones en torno a la protección de datos personales.

El PLAN DE TRABAJO incluyó un cronograma que calendarizó, de manera general, las actividades y/o gestiones que debían realizarse con el propósito de materializar las medidas de seguridad, teniendo como referencia una periodicidad semestral para que la UGTSIJ rindiera informes de avance y cumplimiento ante el Comité de Transparencia.

Es importante recapitular que, en el primer semestre, se reportó la implementación y/o avance de las siguientes actividades:

Rubro de la actividad	2020	
	Semestre 1	Semestre 2
Programa de capacitación institucional		
Pertinencia de tratamientos		
Registro de personal que interviene en tratamientos		
Declaración de confidencialidad		
Registro de responsables de seguridad		
Protección de archivos físicos y electrónicos		
Transferencia de datos		

Fuente: Plan de Trabajo en materia de protección de datos personales

Algunas actividades relacionadas con los rubros “Pertinencia de tratamientos” y “Protección de archivos físicos y electrónicos”, siguen en proceso de implementación y fueron planeadas para ambos semestres del 2020. Incluso, la segunda se extiende al primer semestre de 2021, de acuerdo con la calendarización del PLAN DE TRABAJO, tal como se detallará en el *primer apartado*.

En el informe del primer semestre también se indicó la necesidad de evaluar el fortalecimiento del equipo encargado de la protección de datos personales a nivel institucional, ya que los trabajos se complejizan si consideramos que, además de la implementación del PLAN DE TRABAJO (que incluyen mecanismos de monitoreo y revisión),

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

el Documento de Seguridad está en constante actualización y deben realizarse las medidas necesarias para nivelar aquellos tratamientos que sean incorporados.

Para el segundo semestre de 2020, las medidas de seguridad planeadas fueron las siguientes:

Rubro de la actividad	2020	
	Semestre 1	Semestre 2
Programa de capacitación institucional		
Protección de archivos físicos y electrónicos		
Pertinencia de tratamientos		
Bitácora de vulneraciones		
Bitácora de consulta		
Seguridad informática		

Por lo anterior, en el *segundo apartado* se presentan avances y resultados de aquellas actividades que se informaron en el primer semestre y que continuaron trabajándose durante el periodo que se informa.

En el *tercer apartado* se detallan las medidas implementadas a lo largo del segundo semestre, por orden cronológico. Todas las medidas de seguridad recomendadas a las áreas se realizaron bajo una visión de autorresponsabilidad, de modo que la UGTSIJ recomienda su implementación y son las áreas las que resguardan las evidencias y/o sus productos.

Además, el apartado tercero hace una relatoría sobre las medidas complementarias que la UGTSIJ realizó de manera adicional y paralela al PLAN DE TRABAJO, encaminadas, por un lado, a la atención de los tratamientos de datos personales sensibles derivados de la emergencia sanitaria generada por el virus SARS-CoV2 (COVID-19) y, por otro lado, a la actualización y atención de nuevos tratamientos y/o avisos de privacidad.

Finalmente, en las *conclusiones* se anuncia que en 2021 sucederá el término de la primera etapa del PLAN DE TRABAJO y el comienzo de la segunda, de manera que se apuntan algunas consideraciones para transitar adecuadamente entre una y otra etapa y consolidar los avances alcanzados hasta ese momento.

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

2. Seguimiento de actividades del primer semestre.

A. Programa de capacitación institucional

Como medida administrativa, se incorporó en el PLAN DE TRABAJO una oferta de capacitación especializada al personal involucrado en el tratamiento de los datos personales. En ese sentido, se diseñó el *Programa Anual de Capacitación 2020 (ANEXO 1)*, que incluyó una línea de acción en ese rubro y fue aprobado por el Comité de Transparencia el pasado 12 de febrero de 2020 (en el primer informe se señaló que la implementación de dicha capacitación estaba planeada para realizarse en el segundo semestre de 2020).

En ese sentido y bajo las premisas institucionales encaminadas a proteger la salud, propiciar un entorno seguro que reduzca los riesgos asociados a la enfermedad COVID – 19 y prevenir su transmisión ante la contingencia sanitaria, fue necesario reformular las estrategias para el cumplimiento de las líneas de acción del programa de capacitación, motivo por el cual se gestionaron licencias del software Prezi, que contribuyeron a construir contenidos digitales especializados en la materia y potenciar el alcance de la capacitación.

Por lo anterior, se diseñaron y elaboraron tres cápsulas informativas en torno a las generalidades de la protección de datos personales, las cuales se titulan como sigue:

- “Conceptos clave”, disponible en el siguiente enlace electrónico: <https://prezi.com/v/eeacreyqox8b/>
- “Principios”, disponible en el siguiente enlace electrónico: <https://prezi.com/v/cuxfribyf-jh/>
- “Recepción de datos personales”, disponible en el siguiente enlace electrónico: <https://prezi.com/v/bmcfmwfef8ey/>

El universo de capacitación fueron las personas designadas como responsables de seguridad y 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.

De esta manera, a través de los responsables, se solicitó que dicho personal consultara los contenidos de las cápsulas informativas para homologar los conocimientos generales en materia de datos personales y, al mismo tiempo, consolidar la cultura institucional de su

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

debida protección; además, se atendieron dudas y comentarios sobre estos temas de manera personalizada.

B. Protección de archivos físicos y electrónicos

La protección de archivos físicos y electrónicos incluye, entre otras, las siguientes medidas de seguridad administrativas:

- Clasificación de los archivos.
- Depuración y borrado seguro de los archivos.

Durante el primer semestre, la UGTSIJ impulsó el proyecto para definir un procedimiento institucional de borrado seguro de los datos personales en la institución. En ese sentido, la UGTSIJ colaboró con el Centro de Documentación y Análisis, Archivos y Compilación de Leyes (CDAACL) para promover que las directrices institucionales de archivo administrativo incluyeran estas referencias.

Se advirtió que, para concretar las medidas de seguridad del PLAN DE TRABAJO, era necesario compatibilizar el Catálogo de Disposición Documental (CADIDO) con el Inventario de Tratamientos de Datos Personales, con la finalidad de generar certeza sobre el ciclo de vida a que deben estar sujetos los archivos (físicos y electrónicos) que contienen datos personales.

De esta manera, en la coyuntura de la confección y presentación de una propuesta de acuerdo relativo a la organización, conservación, administración y preservación homogénea del archivo administrativo (pendiente de aprobación), la UGTSIJ colaboró con el CDAACL para que las disposiciones contenidas en dicha propuesta 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.

Asimismo, para desdoblarse dichas propuestas, se intervinieron diversos documentos que darán sentido a las disposiciones del acuerdo: generador de formatos e inventarios documentales, formato de dictamen de baja documental, guía práctica para la organización y resguardo de documentos y expedientes electrónicos y procedimiento de baja documental.

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

C. Pertinencia de tratamientos

Aunque no es una medida de seguridad en particular, el análisis de la pertinencia de los tratamientos se incluyó en el cronograma general del PLAN DE TRABAJO porque era necesario brindar atención especializada a diversos tratamientos que así lo requerían, incluso antes de implementar medidas de seguridad más complejas.

De las actividades señaladas en el primer informe, las únicas que quedaron pendientes son las que a continuación se detallan.

Área	Tratamiento	Atención que requiere	Avance
DGRM	Contratos	Incorporar cláusula de protección de datos personales en contratos institucionales.	Se confeccionó un documento de trabajo, en conjunto con la DGAJ, en donde se señala la pertinencia de regular en los contratos institucionales la relación entre responsable y encargado. Una vez que se valide por la DGAJ, será presentada a las áreas respectivas para avanzar en su implementación (ANEXO 2).
DGIF			
DGCCJ			
DGAJ			
DGTI	Protocolos de actuación	Eliminar la recopilación de datos personales para la descarga de los documentos y eliminar las bases de datos.	Se dialogó con el responsable en turno de la DGDH sobre la pertinencia de eliminar dicho requerimiento en la página. Está pendiente una decisión al respecto.

3. Principales resultados segundo semestre (julio – diciembre 2020)

A. Bitácora de vulneraciones

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

Respecto a esta bitácora, se confeccionó una propuesta en términos de los artículos 37, 38, 39 y 40 de la Ley General en la materia, para un adecuado control y registro de las vulneraciones de datos personales (en particular) o bases de datos y/o sistemas que los

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

albergan (en general), así como para implementar oportunamente acciones preventivas y correctivas con el propósito de evitar que alguna vulneración afecte a más titulares y/o se repita.

Finalmente, la UGTSIJ divulgó el *Instructivo para registrar y reportar vulneraciones de datos personales (ANEXO 3)*, al cual se anexó un *Modelo de Bitácora de Vulneraciones de Datos Personales* 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.

B. Bitácora de consulta

Por lo que hace a la bitácora de consulta y con la finalidad de construir una propuesta institucional que tome como referencia las prácticas implementadas, la UGTSIJ solicitó información a las áreas que efectúan bitácoras para registrar quién accede y consulta las bases de datos personales.

De acuerdo con el PLAN DE TRABAJO, dicho modelo debe contener, cuando menos, nombre y cargo de quien accede a la base de datos; identificación de la información consultada; propósito del acceso; fecha y hora del acceso; y, fecha y hora de devolución.

C. Seguridad informática

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.

En ese sentido, esta UGTSIJ y la Dirección General de Tecnologías de la Información (DGTI), elaboraron y difundieron la *Guía de seguridad informática para la protección de los datos personales (ANEXO 4)*, cuyos propósitos fundamentales son:

- 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.

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

Dicho documento integra recomendaciones y medidas de seguridad en materia informática para que los servidores públicos 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.

4. Medidas complementarias al PLAN DE TRABAJO.

En paralelo a la implementación del PLAN DE TRABAJO, la UGTSJ realizó diversas actividades relacionadas con el fortalecimiento de la política institucional en materia de protección de los datos personales bajo resguardo de la SCJN.

A. Recomendaciones para los tratamientos de datos personales relacionados con la emergencia sanitaria por COVID-19

El Acuerdo General de Administración II/2020 que establece los lineamientos de seguridad sanitaria durante la emergencia generada por el virus SARS-CoV2 (COVID-19) determinó, entre otras cosas, que los datos personales que se recaben por las áreas conforme a esa normativa y la Guía Operativa, serán estrictamente protegidos y tratados en términos de la Ley General de la materia.

Ambos documentos reconocen una serie de medidas que debían observar las áreas para la programación de actividades presenciales, así como obligaciones relacionadas con la comunicación de diagnósticos confirmados positivos de COVID-19 o síntomas asociados a dicha enfermedad. En ese sentido y por sus propias características, la materialización de estos deberes se considera 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 (ANEXO 5)*, 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.

Las citadas recomendaciones aluden diversos documentos orientadores que la propia UGTSIJ ha elaborado y difundido entre aquellas áreas administrativas que tratan datos

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

personales en sus actividades cotidianas, en el marco de la implementación del PLAN DE TRABAJO:

- Guía de protección de datos personales;
- Guía básica para las personas que intervienen en el tratamiento de datos personales;
- Guía para la transmisión segura de datos personales; e,
- Instructivo para registrar y reportar vulneraciones de datos personales.

Como resultado, 24 áreas reportaron tratamientos relacionados con la emergencia sanitaria por el virus SARS-COV-2 (COVID-19).

B. Actualización del Inventarios de Tratamientos

Una consideración adicional en el PLAN DE TRABAJO fue la actualización del inventario de tratamientos de datos personales para revisar que se cumplan cabalmente con los principios de licitud, finalidad, calidad y proporcionalidad en los tratamientos.

Esto implicaría que se incorporen nuevos tratamientos de datos personales que no se habían contemplado en un inicio; que algunos tratamientos registrados sean modificados en su alcance y/o proceso; y, en su caso, que algunos tratamientos deban ser eliminados.

En la primera versión del inventario de tratamientos, anexo al Documento de Seguridad, se reportaron 80 tratamientos registrados, correspondientes a 21 áreas u órganos de la SCJN.

En la actualización anual, dicho inventario reporta 121 tratamientos registrados, correspondientes a 24 áreas u órganos de la SCJN (**ANEXO 6**).

C. Portal de protección de datos personales (sistema de gestión).

En el PLAN DE TRABAJO se estimó viable la modernización de los procesos en los tratamientos de datos personales que permitiera, por ejemplo, la utilización de herramientas software adecuadas para los diversos tratamientos y la automatización en los procesos.

Además, el artículo 34 de la Ley General de la materia, establece que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

deberán estar documentadas y contenidas en un sistema de gestión. Por sistema de gestión, la propia ley entiende al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar mantener y mejorar el tratamiento y seguridad de los datos personales.

Por su parte, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (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 debe contar, cuando menos, con los avisos de privacidad e información relevante en materia de protección de datos personales. Dicho apartado servirá para rendir cuentas del cumplimiento de las obligaciones en el rubro, tanto a los titulares, como al propio INAI.

Previamente y como iniciativa de la UGTSIJ se comenzó a gestar, en coordinación con la DGTI, un espacio en el portal institucional destinado a la protección de datos personales. Este proyecto es más ambicioso que la obligación referida en el Acuerdo del párrafo que antecede, buscando consolidarse, en su momento, como el sistema de gestión.

La propuesta inicial de contenidos se compone de los siguientes elementos (**ANEXO 7**):

- Cápsulas de capacitación;
- Documentos relevantes;
- Gestión de medidas de seguridad;
- Avisos de privacidad;
- Ejercicio de derechos ARCO;
- Normativa en la materia; y,
- Contacto de la Unidad General de Transparencia.

A la fecha, la DGTI se encuentra liberando los códigos para comenzar a cargar los contenidos que defina la UGTSIJ.

5. Conclusiones

Segundo informe semestral UGTSIJ – datos personales

agosto – diciembre 2020

Conforme a la calendarización programada en el PLAN DE TRABAJO, las medidas de seguridad que hasta el momento debían implementarse, están materializadas o en proceso de materializarse. En el primer semestre del año 2021, se estima concluir la primera etapa (ver Proyección Anual, **ANEXO 8**) y comenzar a gestar la segunda etapa dedicada a confeccionar los mecanismos de monitoreo y revisión.

Sin embargo, para transitar exitosamente entre una etapa y otra, es necesario profundizar sobre algunas evidencias en los meses venideros para navegar a buen puerto en la materia.

La primera es publicar y perfeccionar el *sistema de gestión* que se alojará en el portal de protección de datos personales. La misión de esta plataforma es servir como medio para que las áreas puedan autogestionar sus indicadores y sus medidas de seguridad aplicables para sus tratamientos registrados o nuevos y tenerlos actualizados sin necesidad de requerírseles mediante oficio por parte de la UGTSIJ.

Se estima que esta propuesta debe ser el cigoto de un proyecto más ambicioso, que implica software especializado en la gestión de protección de datos personales a nivel institucional.

Por otra parte, sigue siendo necesario perfilar un grupo de personas encargado del tema de protección de datos personales con atribuciones en el rubro. Como se informó en el Documento de Seguridad, la UGTSIJ no cuenta con el personal adscrito exclusivamente a dichas tareas, en tanto su creación se dio en el contexto de la Ley General de Transparencia y Acceso a la Información Pública y solo tomó en consideración dichas obligaciones.

Las tareas en torno al tema se complejizarán en la medida que se dejará la etapa de implementación de medidas de seguridad y las actividades se enfocarán en el monitoreo, revisión y actualización de todos los insumos hasta ahora implementados, en específico de todos los que integran el Documento de Seguridad y los procesos de mejora.