Plan de trabajo en materia de protección de datos personales

Suprema Corte de Justicia de la Nación

Unidad General de Transparencia y
Sistematización de la Información Judicial

Versión: noviembre 12 de 2019

Plan de trabajo en materia de protección de datos personales
SCJN 2020-2022

I. Presentación

A propuesta de la Unidad General de Transparencia y Sistematización de la Información Judicial (UGTSIJ), el pasado 11 de septiembre de 2019, el Comité de Transparencia de la Suprema Corte de Justicia de la Nación (SCJN), aprobó el Documento de Seguridad institucional en su décima sesión pública extraordinaria.

Además, en términos de los artículos 35 fracción V y 84 fracciones IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), instruyó a la propia UGTSIJ para que elaborara un plan de trabajo relacionado con los hallazgos del Documento de Seguridad.

Es importante recapitular que el Documento de Seguridad ofrece una radiografía institucional en materia de protección de los datos personales en su faceta administrativa; refleja sus fortalezas, pendientes y áreas de oportunidad; y, constituye un insumo para la toma de decisiones por parte de las instancias competentes en ese renglón.

En función de las particularidades que revela dicho instrumento, es posible obtener información sobre necesidades específicas de la SCJN para el diseño de planes de trabajo; así como la implementación y factibilidad de mecanismos de monitoreo y revisión de medidas de seguridad, que también integran el Documento de Seguridad y son imprescindibles para que el Comité de Transparencia disponga lo conducente en torno a estas medidas institucionales.

Derivado de lo anterior, la UGTSIJ perfiló el presente Plan de Trabajo como una herramienta complementaria y de instrumentalización del Documento de Seguridad previamente aprobado por el Comité de Transparencia, cuyos objetivos fundamentales son 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.

Las actividades encaminadas al cumplimiento de dichos objetivos se realizarán y/o coordinarán por la UGTSIJ bajo las directrices que guiaron la elaboración del Documento de Seguridad: *i)* con acciones de carácter orientativo, *ii)* acudiendo a los deberes institucionales que prevé la Ley General; y, *iii)* priorizando la colaboración entre las áreas administrativas de la SCJN.

Al respecto, es importante considerar que la creación UGTSIJ se presentó en el contexto de la reforma constitucional de 2014 en materia de transparencia y teniendo como referencia únicamente las disposiciones previstas en la Ley General de Transparencia y Acceso a la Información Pública, de ahí que el Reglamento Orgánico en Materia de Administración de este Alto Tribunal únicamente prevé atribuciones en ese renglón.

Por ello y en paralelo al despliegue de dichas actividades, en aras del cumplimiento de las metas trazadas en este Plan de Trabajo, es pertinente evaluar la creación de un área determinada o una instancia de coordinación –integrada por representantes de distintas áreas– encargada del seguimiento de las acciones emprendidas para el cumplimiento de las obligaciones emanadas de la Ley General.

En ese sentido, el Plan de Trabajo contempla un trabajo de tres años que marcarán el término de la administración a cargo de la Presidencia del Ministro Arturo Zaldívar Lelo de Larrea y se implementarán en dos etapas que

se condicen con los propios objetivos: *i)* eliminar las brechas en las medidas de seguridad; e, *ii)* implementar mecanismos de monitoreo.

Debido a que ambas etapas implican desarrollar insumos, herramientas y estrategias para ejecutar acciones concretas, así como coordinar esfuerzos con diversas áreas de este Alto Tribunal, el periodo de cumplimiento es genérico, de 18 meses a 24 meses la primera de ellas, y de 18 meses la segunda.

Por otro lado, resulta importante mencionar que el presente Plan de Trabajo se concilió previamente con aquellas áreas involucradas en acciones en donde su participación resulta necesaria para ser ejecutadas.

En concreto, el pasado 10 de octubre se celebró una reunión en la que estuvieron presentes las personas titulares del Centro de Documentación y Análisis, Archivos y Compilación de Leyes, la Dirección General de Tecnologías de la Información y la Dirección General de Seguridad, quienes conocieron las actividades de este plan que les involucra, compartieron sus opiniones y lo retroalimentaron en aras de una participación adecuada durante su ejecución.

II. Primera Etapa

- **OBJETIVO:** implementar las medidas de seguridad recomendadas para los tratamientos de datos personales
- **PLAZO:** 18 a 24 meses

Esta etapa tiene como propósito fundamental eliminar las brechas en los tratamientos de datos personales identificados en la SCJN, de manera que los recursos se dirigirán para que las medidas de seguridad recomendadas sean implementadas o, en su caso, se encuentren en vías de implementación dentro del periodo en que se desarrollará.

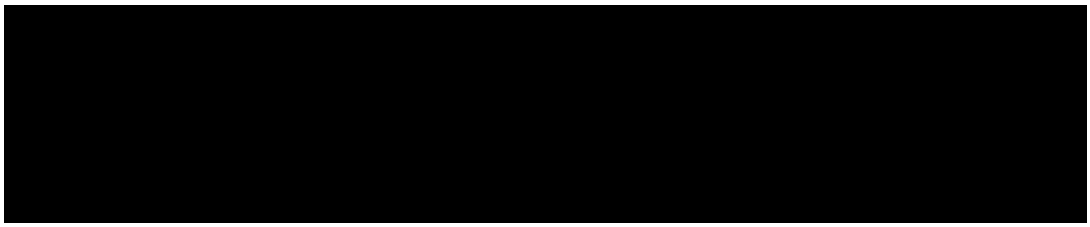
Al respecto, debe considerarse que el Documento de Seguridad contempla un *análisis de brecha* que identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados por las áreas administrativas de la SCJN.

Como medida previa a este análisis, se confeccionó un Catálogo de Medidas de Seguridad para los tratamientos de datos personales, el cual consideró 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 en la parte conducente.

En ese documento se describen las medidas de seguridad administrativas, físicas y técnicas –complementarias a las políticas de seguridad generales de la SCJN– para los tratamientos de datos personales en la institución.

Además, se incluyen recomendaciones generales de medidas de seguridad para cada tratamiento, tomando como referencia el nivel de riesgo latente que fue reportado.

Lo principales resultados del *análisis de brecha*, arrojaron lo siguiente:



Por tanto, la meta para esta primera etapa tiene como propósito que todos los tratamientos de datos personales tengan un cumplimiento cercano al 100% de las medidas de seguridad recomendadas.

Se estima que el cumplimiento de la meta fijada para la primera etapa se concrete en un plazo de entre 18 y 24 meses, a partir de enero de 2020. Es decir, entre julio y diciembre de 2021, la primera etapa deberá estar consolidada.

Para ello, este documento presenta, como una primera aproximación a la ejecución de esta etapa, una serie de actividades cuya descripción se incorpora en la matriz del apartado siguiente, la cual incluye cada una de las medidas de seguridad identificadas, el insumo necesario para cumplirlas y el área o áreas involucradas, según sea el caso.

Es necesario advertir sobre la importancia de generar esquemas de trabajo interdependientes con aquellas áreas que juegan un papel trascendental en la protección de los datos personales a nivel institucional y que están involucradas en la generación de las políticas, acciones y medidas que se describen más adelante.

II.I. Programación.

En este apartado se desarrollan las implicaciones relacionadas con la implementación de las medidas de seguridad recomendadas para los tratamientos de datos personales, de conformidad con el Catálogo de Medidas de Seguridad previsto en el Documento de Seguridad.

En el apartado de áreas responsables, se prevé la intervención conjunta entre la UGTSIJ y las Direcciones Generales de Tecnologías de la Información (DGTI), de Seguridad (DGS), de Recursos Materiales (DGRM), de Infraestructura Física (DGIF) y el Centro de Documentación, Análisis, Archivo y Compilación de Leyes (CDAACL), según corresponda.

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

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
Declaración de confidencialidad	**Administrativa**	Realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.	1. Modelo institucional de declaración de confidencialidad, que deberán firmar las personas involucradas en el tratamiento de datos personales 2. Guía para el tratamiento de los datos personales, acordes a los principios que marca la ley	UGTSIJ

Plan de trabajo en materia de protección de datos personales
SCJN 2020-2022

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
Listado de personal que interviene en el tratamiento de datos	**Administrativa**	Elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales que incluya, entre otros, nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.	1. Modelo de listado de personal responsable, a efecto de que se contemple qué personas tienen relación con los tratamientos. 2. Base de datos de servidores públicos responsables de tratamiento.	UGTSIJ
Clasificación de los archivos físicos	**Administrativa**	Identificar, valorar y, en su caso, incluir en el Catálogo de Disposición Documental los expedientes de archivo que incorporan documentos que reflejan tratamientos de datos personales, con la finalidad de generar certeza sobre el ciclo de vida a que deben estar sujetos.	1. Política de actualización y depuración de los archivos físicos administrativos. 2. Políticas internas para el tratamiento y ciclo de vida de los archivos electrónicos administrativos. 3. Versión del Catálogo de Disposición Documental vinculado a los expedientes de archivo que incorporan documentos que reflejan tratamientos de datos personales. 4. Modelo de procedimiento y acta para la constancia del borrado de bases de datos personales.	CDAACL UGTSIJ DGTI
Clasificación de los archivos electrónicos	**Administrativa**	Identificar y etiquetar las bases de datos (soporte electrónico) relacionadas con tratamientos de datos personales con un nombre que así las identifique, conforme al inventario reportado por el área. Eventualmente, definir si esas bases de datos deberían integrarse a los instrumentos archivísticos		
Depuración y borrado seguro del archivo físico	**Administrativa**	Implementar un programa de depuración documental respecto de los expedientes de archivo que incorporan documentos que reflejan tratamientos de datos personales, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.		
Depuración y borrado seguro del archivo electrónico	**Administrativa**	Implementar un programa de borrado –seguro y permanente– de las bases de datos o parte de ellas, que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo. Una posibilidad es el borrado integral de la información o, en su defecto, reinicio de los		

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
		equipos o medios de almacenamiento a los valores de origen. Además, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la UGTSIJ.		
Capacitación	**Administrativa**	Incorporar oferta de capacitación especializada al personal involucrado en el tratamiento de los datos personales.	Proponer, aprobar e implementar el Programa de Capacitación 2020, con perspectiva de protección y medidas de seguridad de datos personales, mismo que incluya los siguientes cursos: 1. Virtuales a través del CEVINAI en materia de datos personales. 2. Otorgados por la UGTSIJ, sobre: i) el rol de los enlaces en materia de protección de datos personales y su actividad a la luz del plan de trabajo; ii) las obligaciones de aquellas personas que recaban, de primera mano, datos personales (personal encargada de registro de visitas y atención médica). 3. Sobre cuidados de bienes informáticos y medidas de seguridad básicas en espacios físicos que resguardan datos personales, coordinado por la DGTI y la DGS. 4. En materia de archivos, relacionados con medidas de seguridad.	UGTSIJ DGTI DGS CDAACL

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
Bitácora de vulneraciones	**Administrativa**	Implementar un control informativo en donde se reporten los tipos de vulneraciones con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la UGTSIJ para que tome las acciones pertinentes. Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.	1. Guía para registrar y reportar vulneraciones. 2. Modelo de Bitácora, que contenga, al menos, los siguientes datos: - Nombre y cargo de quien reporta el acceso/ vulneración - Fecha y hora del acceso/ vulneración - Motivo(s) del acceso/vulneración - Acciones correctivas - Acciones preventivas	UGTSIJ
Bitácora de consulta	**Administrativa**	Establecer una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.	1. Modelo de bitácora que contenga, al menos, los siguientes datos: - Nombre y cargo de quien accede a la base de datos - Identificación de la información consultada - Propósito del acceso - Fecha y hora del acceso - Fecha y hora de devolución	UGTSIJ
Responsable de seguridad	**Administrativa**	Designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.	1. Responsable de seguridad en cada área que trate datos personales, con el fin de que se preserven y haya una comunicación directa con la UGTSIJ.	UGTSIJ

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
			En aquellas áreas con tratamientos sensibles, el responsable deberá ser persona diferente al enlace de transparencia. 2. Decálogo del responsable de seguridad.	
Transferencias	**Administrativa**	Realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.	1. Guía para realizar transferencias.	UGTSIJ
Cuidado de los bienes informáticos	**Física**	Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por la Dirección General de Tecnologías de la Información, tampoco alterar el orden de los cables conectados.[1]	1. Implementación de una política institucional en materia de seguridad informática que incluya, al menos, lo siguiente: - Materiales didácticos; - Mecanismos de difusión masiva;y, - Ajustes normativos.	DGTI UGTSIJ
No instalar equipos ajenos	**Física**	Abstenerse de instalar equipos de cómputo que no sean propiedad de la SCJN sin permiso de la Dirección General de Tecnologías de la Información. Los usuarios que requieran hacer uso de la red interna de SCJN deben usar solamente las direcciones IP asignadas por el área administrativa correspondiente. En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus. En el caso de		

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

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
		encontrarse infectado el dispositivo, el usuario debe extraer inmediatamente sin consultar, modificar o copiar información alguna.		
Cuidado de la contraseña personal	**Técnica**	Abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático de la SCJN.		DGTI DGS UGTSIJ
Actualización de contraseñas	**Técnica**	Cambiar las contraseñas cada tres meses por lo menos, a efecto de evitar robo de identidad. En caso de olvido o sospecha de divulgación de una contraseña o mecanismo de autenticación, los usuarios deberán realizar el cambio de los mismos en los sistemas informáticos de la SCJN.		
Reportar fallas	**Técnica**	Notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.		
No instalar softwares	**Técnica**	Abstenerse de descargar en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.		
Contraseñas robustas	**Técnica**	Construir contraseñas con rol de administrador de forma robusta, atendiendo a los siguientes criterios: - Contar con una longitud mínima de 12 caracteres. - Incluir, por lo menos, dos letras mayúsculas, dos letras minúsculas, dos símbolos especiales (punto, coma, guion, etcétera) y un número; - Evitar el uso de palabras comunes o datos personales; - Renovarlas de manera periódica;		

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
		- Las contraseñas no podrán repetirse en al menos 10 iteraciones; - Almacenarlas de forma cifrada y en archivos electrónicos distintos en los que se almacenan datos de aplicaciones.		
Respaldo de información	**Técnica**	Realizar respaldos de la información que resida en el equipo de cómputo asignado. La Dirección General de Tecnologías de la Información, a solicitud del usuario, asesorará y apoyará a los usuarios en el procedimiento para considerando las necesidades propias del área.		
Prevenir accesos no autorizados	**Física**	Prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.	* Estas medidas de seguridad serán cubiertas por la capacitación respectiva (curso 3).	DGS UGTSIJ
Traslado de equipos de cómputo	**Física**	Observar los procedimientos dispuestos para el traslado de equipos de cómputo fuera de las instalaciones de la SCJN.		
Archivero con candado	**Física**	Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado. Derivado del inventario, se detectan tratamientos que lo requieren.	1. Modelo de verificación para aquellos archivos físicos con datos personales que lo requieran.	UGTSIJ DGRM
Candados de seguridad para equipos de cómputo	**Física**	Fijar con candados de seguridad los equipos de cómputo que contengan bases de datos personales.	1. Modelo de verificación sobre la implementación de estas medidas.	UGTSIJ
Zona de confidencialidad	**Física**	Definir una zona de confidencialidad en donde se resguardarán los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el	1. Dictamen conjunto para determinar qué áreas deben implementar zona de confidencialidad.	DGIF DGRM

Tipo de medida	Categoría	Descripción	Insumos/formas de implementación	Áreas involucradas
		acceso al personal no autorizado, equipos o aparatos de copiado.	2. Zonas de confidencialidad en las áreas que lo requieran, a través de dispositivos biométricos, tarjetas inteligentes, puertas con control de acceso.	UGTSIJ

II.II. Consideraciones adicionales.

En paralelo al cumplimiento de las metas programadas, se estima necesario durante esta etapa actualizar el inventario de tratamientos de datos personales, para revisar que se cumplen cabalmente con los principios de licitud, finalidad, calidad y proporcionalidad en los tratamientos.

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

Además, resulta necesario hacer una revisión de los contratos a través de los cuales se comparten datos personales a terceros, para recomendar la implementación de cláusulas claras sobre protección y responsabilidad en el tratamiento de los mismos.

Finalmente y como un mecanismo de monitoreo, la UGTSIJ rendirá informes semestrales al Comité de Transparencia en los que dé cuenta del avance de cumplimiento del presente Programa de Trabajo, así como de las novedades o cuestiones adicionales que estime conveniente hacer de su conocimiento para contemplarlas en los esfuerzos institucionales.

III. Segunda etapa

- **OBJETIVO:** definir e implementar mecanismos de monitoreo y revisión
- **PLAZO:** 18 meses

Esta etapa tiene 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.

Para ello, será necesario generar esquemas de revisión de cumplimiento de las medidas de seguridad en todos los tratamientos de acuerdo al nivel de riesgo, en la que sea posible integrar a todas las áreas involucradas que tratan datos personales.

Es importante tomar en consideración las áreas de oportunidad que se revelen en la implementación de esta segunda etapa, para mejorar los procesos en el tratamiento y en la protección de los datos personales.

La última etapa será desarrollada en los últimos 18 meses del periodo en que está programado el presente Plan de Trabajo. Es decir, en diciembre de 2022, la segunda etapa deberá estar consolidada.

III.I. Programación.

- Monitoreos

Los monitoreos se programan de tal forma que sea posible concluir las acciones previstas en la primera etapa; por tanto, se considera que las medidas de seguridad recomendadas para aquellos tratamientos con riesgo

bajo estarán listas para revisarse y evaluarse en los primeros momentos de los segunda etapa, lo que puede no suceder con aquellas medidas más complejas y dirigidas a los tratamientos con riesgo alto.

Esta programación no implica desatender el acompañamiento para la implementación de todas las medidas de seguridad.

Monitoreo	Descripción	Criterios de evaluación
Tratamientos con riesgo bajo	Se realizarán monitoreos de cumplimiento de medidas de seguridad de aquellos tratamientos que registraron un riesgo según el análisis respectivo. El monitoreo deberá ser coordinado por la UGTSIJ, en conjunto con la DGTI, DGS, DGRM y DGIF.	Censo para la revisión de las medidas de seguridad administrativas, físicas y técnicas, con evidencia de cumplimiento que respalde las respuestas de las áreas.
Tratamientos con riesgo medio		
Tratamientos con riesgo alto		

Como un mecanismo de monitoreo, la UGTSIJ también rendirá informes semestrales al Comité de Transparencia en los que dé cuenta del avance de cumplimiento del presente Programa de Trabajo, así como de las novedades que estime conveniente hacer de su conocimiento.

En su último informe, la UGTSIJ realizará una actualización del análisis de brecha previsto en el Documento de Seguridad para contrastar los resultados obtenidos en la implementación de este Plan de Trabajo (2022) con aquellos registrados inicialmente en aquel documento (2019).

IV. Consideraciones finales

Como medidas complementarias en el cumplimiento de este Plan de Trabajo y en aras de la consolidación de una política institucional de protección de datos personales, se vislumbran dos rutas relacionadas con la apertura y modernización de procesos.

Se considera factible que la revisión de la seguridad y protección de los tratamientos de datos personales se acompañe de la asesoría y colaboración de autoridades, organizaciones o terceros ajenos a la SCJN, especializados en el tema, con el objeto de fortalecer el parámetro de cumplimiento en la materia, en una suerte de ejercicio de gobierno abierto (justicia abierta, para el caso de este Alto Tribunal).

Además, se estima viable la modernización de los procesos en los tratamientos de datos personales que permita, por ejemplo, la utilización de herramientas software adecuadas para los diversos tratamientos y la automatización en los procesos de manera que permitan la trazabilidad de los datos personales, así como su sistematización, disociación y portabilidad, entre otros beneficios que redundan en la seguridad de éstos.

V. Cronograma General

El cronograma busca calendarizar, de manera general, las actividades y gestiones que deben llevarse a cabo para materializar en tiempo y forma el presente Plan de Trabajo, tomando como base la periodicidad semestral en que la UGTSIJ debe rendir informes de avance y cumplimiento al Comité de Transparencia. Es necesario advertir que, debido a que el Plan de Trabajo es de largo alcance, esta proyección debe interpretarse con la posibilidad de que se presenten pormenores o complicaciones no previstas y que impacten en la modificación de los tiempos de cumplimiento.

CRONOGRAMA GENERAL / PLAN DE TRABAJO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES						
Rubro de la actividad	**2020**		**2021**		**2022**	
	Semestre 1	Semestre 2	Semestre 1	Semestre 2	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						
Bitácoras de vulneraciones y consulta						
Transferencia de datos						
Seguridad informática						
Proyección anual						

Protección física de los datos personales						
Monitoreo para tratamientos con riesgo bajo						
Monitoreo para tratamientos con riesgo medio						
Monitoreo para tratamientos con riesgo alto						
Segundo análisis de brecha						

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

Fecha de clasificación	17 de febrero de 2020.
Área	Secretaría del Comité de Transparencia
Documento	Plan de Trabajo en materia de protección de datos personales
Tipo de clasificación	Reserva parcial respecto de las medidas de seguridad en materia de datos personales y la forma de ejecución
Fundamento legal	El artículo 113, fracciones I y VIII de la Ley General de Transparencia y Acceso a la Información Pública en relación con diverso 110, fracciones I y VII de la Ley Federal de Transparencia y Acceso a la Información Pública
Observaciones	Se suprime en **color negro** las medidas de seguridad en materia de datos personales y la forma de ejecución
Firma del titular	**Ariel Efrén Ortega Vázquez** **Secretario del Comité de Transparencia**