TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

DOCUMENTO DE SEGURIDAD DEL TRIBUNAL ELECTORAL DEL PODER JUDICIAL DE LA FEDERACIÓN

2020

Índice

PRESENTACIÓN 3

I. OBJETIVO 5

II. MARCO NORMATIVO 6

III. GLOSARIO 7

IV. INVENTARIOS DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO 11

V. FUNCIONES Y OBLIGACIONES DEL PERSONAL QUE TRATE DATOS PERSONALES 20

VI. ANÁLISIS DE RIESGO 28

VII. ANÁLISIS DE BRECHA 37

VIII. PROGRAMA GENERAL DE CAPACITACIÓN 43

IX. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD. 45

PRESENTACIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1] tiene como 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 cualquier autoridad, entidad, órgano y organismo del ámbito federal, estatal y municipal, de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Dentro de las obligaciones que esta Ley prevé, se encuentra el deber de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, detección o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.[2]

Por ello, en febrero de 2019, el Comité de Transparencia y Acceso a la Información del Tribunal Electoral del Poder Judicial de la Federación aprobó, en cumplimiento del deber de seguridad previsto en los artículos 31 al 34 del citado ordenamiento y 55 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad contenía lo siguiente:

- 36 inventarios de tratamiento de datos personales.
- Las funciones y obligaciones de las servidoras públicas y de los servidores públicos que traten datos personales.
- El análisis de riesgo de cuatro de los sistemas: contrataciones de obra pública, accesos y salidas peatonales, accesos y salidas vehiculares, y sistema de circuito cerrado de CCTV.
- El análisis de brecha y el plan de trabajo del sistema de tratamiento de contrataciones de obra pública.

[1] Publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
[2] Artículo 31 de la Ley General de Datos.

- La detección de necesidades de capacitación sobre el sistema de contrataciones de obra pública, accesos y salidas peatonales, accesos y salidas vehiculares, y sistema de circuito cerrado de CCTV.
- Los supuestos de actualización del documento.

Respecto a la actualización del documento, se estableció que de conformidad con el artículo 36 de la Ley General de Datos, debería actualizarse cuando:

- Se produjeran modificaciones sustanciales en el nivel de riesgo.
- Como resultado de un proceso de mejora para mitigar la vulneración a la seguridad ocurrida.
- Fuera el resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión para la seguridad de los datos personales que en su momento se emita para el Alto Tribunal.

Al respecto, es importante mencionar que durante 2019 y 2020, la Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales implementó diversas acciones de monitoreo y mejora continua que derivaron en la actualización de inventarios y avisos de privacidad de todas las áreas administrativas y jurisdiccionales del Tribunal Electoral del Poder Judicial de la Federación; así como en la revisión del documento de seguridad. Advirtiéndose la necesidad de actualizarlo al detectar sistemas de tratamiento que, si bien contaban con la estructura, medidas de seguridad e incluso, en algunos casos avisos de privacidad, los mismos no se encontraban contemplados de manera formal en el documento de seguridad.

Por ello, tras la revisión y trabajo conjunto con cada una de las áreas responsables de coordinar las actividades que conllevan el tratamiento de datos personales, se presenta la actualización del Documento de Seguridad del Tribunal Electoral del Poder Judicial de la Federación.

I. OBJETIVO

El Documento de Seguridad del TEPJF, en cumplimiento al artículo 35 de la Ley General de Datos, tiene por objetivo establecer las medidas de seguridad administrativas, físicas y técnicas mínimas que deberán observar quienes realicen el tratamiento de los datos personales que se encuentren en posesión de este Alto Tribunal; así como el plan de trabajo y de capacitación necesario para garantizar la óptima protección de los datos personales que se encuentran en su poder.

Para ello, el documento contará con los siguientes apartados:

- Objetivo.
- Marco Normativo.
- Glosario.
- Inventarios de datos personales.
- Funciones y obligaciones de las personas que tratan datos personales.
- Análisis de Riesgos.
- Análisis de brecha y Plan de Trabajo.
- Programa General de Capacitación.
- Actualización del documento de seguridad.

Por ello, este documento es de observancia obligatoria para las servidoras públicas y los servidores públicos el TEPJF que realicen algún tipo de tratamiento de datos personales.

II. MARCO NORMATIVO

- Artículo 11 de la Convención Americana Sobre Derechos Humanos.
- Artículos 1, 6, 16 y 99 de la Constitución Política de los Estados Unidos Mexicanos.
- Artículos 1 y del 184 al 186 de la Ley Orgánica del Poder Judicial de la Federación.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Reglamento Interno del Tribunal Electoral del Poder Judicial de la Federación.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Acuerdo General de Administración del Tribunal Electoral del Poder Judicial de la Federación.
- Lineamientos para la Protección Institucional del Tribunal Electoral del Poder Judicial de la Federación.
- Políticas Generales en Materia de Tecnología de la Información del Tribunal Electoral del Poder Judicial de la Federación.
- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales.
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

III. GLOSARIO

Para efectos del presente documento se entenderá por:

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

Área Administrativa: Área a la que se le confieren atribuciones específicas en el Acuerdo General de Administración del Tribunal Electoral del Poder Judicial de la Federación.

Área Jurisdiccional: Área que la conforman la Sala Superior y las Salas Regionales de Guadalajara, Monterrey, Xalapa, Ciudad de México, Toluca, y Especializada que forman parte del Tribunal Electoral del Poder Judicial de la Federación.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, de conformidad con lo establecido en el Título Tercero de la Ley General de Datos.

DGTAIPDP: Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales.

Disponibilidad: Que las personas o procesos autorizados accedan a la información cuando así lo requieran, sin sufrir degradación alguna en cuanto a accesos.

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

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable.

Integridad: garantizar la exactitud y la confiabilidad de la información de manera que no pueda ser modificada sin autorización, ya sea accidental o intencionadamente.

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

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

Medidas de seguridad: consisten en un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organización, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

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

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados,
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del *software* y *hardware,* y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Responsable: Sujeto obligado de la Ley General de Datos que decide el tratamiento de los datos personales.

Soporte: medio de obtención o el formato de almacenamiento, ya sea físico o electrónico, en el que residen los datos personales tratados.

TEPJF: Tribunal Electoral del Poder Judicial de la Federación.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano realizada a persona distinta del titular, del responsable o del encargado.

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

IV. INVENTARIOS DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Para poder verificar el cumplimiento de las obligaciones previstas en el artículo 35, fracción I, de la Ley General de Datos es necesario contar con un diagnóstico de cada uno de los procesos que las áreas competentes realizan el tratamiento de datos personales. Este diagnóstico se realiza a través de la elaboración de un "inventario de sistema de tratamiento", el cual debe formar parte del documento de seguridad.

Para garantizar orden y precisión en el inventario, se deben tener en consideración los elementos mínimos establecidos en los artículos 58 y 59 de los Lineamientos Generales de Datos:

> ***Inventario de datos personales***
> ***Artículo 58.*** *Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
>
> ***I.*** *El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
> ***II.*** *Las finalidades de cada tratamiento de datos personales;*
> ***III.*** *El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
> ***IV.*** *El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
> ***V.*** *La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
> ***VI.*** *En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*
> ***VII.*** *En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*
>
> ***Ciclo de vida de los datos personales en el inventario de éstos***
> ***Artículo 59.*** *Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*
>
> ***I.*** *La obtención de los datos personales;*
> ***II.*** *El almacenamiento de los datos personales;*

> ***III.*** *El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;*
> ***IV.*** *La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;*
> ***V.*** *El bloqueo de los datos personales, en su caso, y*
> ***VI.*** *La cancelación, supresión o destrucción de los datos personales.*
>
> *El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.*

A partir de ello y como parte del proceso de mejora continua, la DGTAIPDP realizó, en coordinación con las áreas administrativas competentes, la revisión de los inventarios de datos personales referidos en el Documento de Seguridad aprobado el pasado 18 de febrero del 2019.

Como resultado de esta revisión se identificó la necesidad de hacer las modificaciones que se desglosan a continuación:

ÁREA ADMINISTRATIVA	DOCUMENTO DE SEGURIDAD FEB-19	REVISIÓN SEPT- 20	AJUSTE
Contraloría Interna	3	4	Incrementó
Defensoría Pública Electoral para Pueblos y Comunidades Indígenas	3	3	Se detectó la duplicidad de un sistema por lo que se eliminó y se adicionó un nuevo sistema
Dirección General de Adquisiciones, Servicios y Obra Pública	2	2	Modificación
Dirección General de Asuntos Jurídicos	2	3	Incrementó

ÁREA ADMINISTRATIVA	DOCUMENTO DE SEGURIDAD FEB-19	REVISIÓN SEPT- 20	AJUSTE
Dirección General de Comunicación Social	1	1	Modificación
Dirección General de Documentación	2	2	Modificación
Dirección General de Igualdad de Derechos y Paridad de Género	1	1	Incrementó
Dirección General de Investigación de Responsabilidades Administrativas	0	1	Incrementó
Dirección General de Jurisprudencia, Seguimiento y Consulta	0	1	Incrementó
Dirección General de Mantenimiento y Servicios Generales	0	4	Incrementó
Dirección General de Planeación y Evaluación Institucional	1	1	Modificación
Dirección General de Protección Institucional	3	2	Se fusionaron dos
Dirección General de Recursos Financieros	2	2	Modificación
Dirección General de Recursos Humanos	2	4	Incrementó
Dirección General de Relaciones Institucionales Internacionales	2	2	Modificación

ÁREA ADMINISTRATIVA	DOCUMENTO DE SEGURIDAD FEB-19	REVISIÓN SEPT- 20	AJUSTE
Dirección General de Relaciones Institucionales Nacionales	1	11	Modificación e incrementó
Dirección General de Sistemas	0	2	Incrementó
Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales	3	4	Incrementó
Escuela Judicial Electoral	4	8	Incrementó
Visitaduría Judicial	1	1	Incrementó
Dirección General de Administración Regional	0	6	Incrementó
Secretarías Generales de Acuerdos	0	10	Incrementó
Secretaría Administrativa	3	0	Decremento
TOTAL:	36	75	

Las modificaciones realizadas a los inventarios reportados durante 2019 tuvieron como base las siguientes razones que se detallan a continuación:

ÁREA ADMINISTRATIVA	NOMBRE DEL TRATAMIENTO REPORTADO EN 2019	OBSERVACIONES
Defensoría Pública Electoral para Pueblos y	Información curricular de defensores	Se eliminó ya que la información correspondía a datos vinculados con otro proceso.

ÁREA ADMINISTRATIVA	NOMBRE DEL TRATAMIENTO REPORTADO EN 2019	OBSERVACIONES
Comunidades Indígenas		
Dirección General de Relaciones Institucionales Nacionales	Concursos y eventos de vinculación	Se modificó y dividió, pues se advirtió que estaban agrupados procesos diversos con finalidades diversas en un sólo inventario.
Escuela Judicial Electoral	Contratación de profesores, ponentes, investigadores, dictaminadores	Se eliminó porque se encontraba duplicado
	Acciones de formación y capacitación	Se modificó y dividió, pues se advirtió que estaban agrupados procesos diversos con finalidades diversas en un sólo inventario.
Secretaría Administrativa	Servicio civil de carrera	Se eliminó ya que aún no se tiene fecha de la aplicación de este tratamiento de datos personales.
	Control interno	Se eliminó pues la información correspondía a datos vinculados con otro proceso.
	Comisión de administración	

ÁREA DEL TEPJF	NOMBRE DEL TRATAMIENTO REPORTADO EN 2019	OBSERVACIONES
Delegaciones Administrativas	Accesos	Estos tratamientos se refirieron en una de las tablas incluidas en el documento de 2019; sin embargo, no se incorporó más
	Servicio médico	
	Circuito cerrado de TV	

de Salas Regionales	Adquisiciones	información ni inventarios, por lo que se trabajó con las unidades competentes y se elaboraron los inventarios respectivos.
	Eventos	
	Relación Laboral	
	Biblioteca	

Así, los inventarios que forman parte integral del presente Documento de Seguridad, se encuentran contenidos en el **Anexo 1** y corresponden a los siguientes tratamientos:

ÁREA ADMINISTRATIVA		NO. INVENTARIOS ENTREGADOS	NOMBRE DEL TRATAMIENTO
1	Contraloría Interna	4	Procedimiento de responsabilidad
			Procedimientos de ejecución de auditoría, revisiones de control, seguimiento de acciones de mejora y evaluación al ejercicio del gasto.
			Proceso para la realización de actas entrega-recepción.
			Sistema de declaraciones de situación patrimonial y de intereses.
2	Defensoría Pública Electoral para Pueblos y Comunidades Indígenas	3	Convocatoria para conformar la lista de personas habilitadas para desempeñarse como defensoras y defensores adscritos a la Defensoría Pública Electoral para Pueblos y Comunidades Indígenas.
			Eventos.
			Solicitud de servicios de asesoría y defensa en materia electoral (SIDEPE).
3	Dirección General de Adquisiciones, Servicios y Obra Pública	2	Procedimientos concursales de adjudicación.
			Procedimientos de adjudicación directa formalizados a través de pedidos, órdenes de compra, de servicio y/o de trabajo.
4		3	Representación y defensa de los intereses del TEPJF.

ÁREA ADMINISTRATIVA		NO. INVENTARIOS ENTREGADOS	NOMBRE DEL TRATAMIENTO
	Dirección General de Asuntos Jurídicos		Elaboración de contratos.
			Elaboración y formalización de convenios.
5	Dirección General de Comunicación Social	1	Coordinación y promoción con medios de comunicación.
6	Dirección General de Documentación	2	Servicios bibliotecarios del Centro de Documentación CENDOC.
			Eventos de difusión y distribución de publicaciones.
7	Dirección General de Igualdad de Derechos y Paridad de Género	1	Actividades de formación, difusión, vinculación o en materia de accesibilidad para personas con discapacidad.
8	Dirección General de Investigación de Responsabilidades Administrativas	1	Investigación de Responsabilidades Administrativas.
9	Dirección General de Jurisprudencia, Seguimiento y Consulta	1	Cursos y talleres de capacitación en materia de tesis y jurisprudencia electoral.
10	Dirección General de Mantenimiento y Servicios Generales	4	Mesa de Servicios de Mantenimiento.
			Sistema de Control Vehicular.
			Sistema de Almacén, Inventarios y Desincorporación.
			Mesa de Servicios de Almacén.
11	Dirección General de Planeación y Evaluación Institucional	1	Mecanismos de participación ciudadana en portal interactivo.
12	Dirección General de Protección Institucional	2	Sistema de circuito cerrado de televisión.
			Sistema de control de acceso (peatonal y vehicular).

ÁREA ADMINISTRATIVA		NO. INVENTARIOS ENTREGADOS	NOMBRE DEL TRATAMIENTO
13	Dirección General de Recursos Financieros	2	Pagos por adquisición de bienes u ordenes de servicio.
			Registros presupuestales y contables.
14	Dirección General de Recursos Humanos	4	Integración de expediente y seguimiento de relación laboral.
			Servicio Médico.
			Servicio de Atención Psicológica.
			Servicio Social.
15	Dirección General de Relaciones Institucionales Internacionales	2	Actividades de vinculación Internacional.
			Solicitud de información para casos de derechos humanos por la Secretaría de Relaciones Exteriores.
16	Dirección General de Relaciones Institucionales Nacionales	11	Visitas Guiadas Externas.
			Visitas Guiadas Familiares.
			Foros Juveniles Presenciales.
			Foros Juveniles Virtuales.
			Taller de Análisis de Sentencias y cine-debate virtual.
			Taller de Análisis de Sentencias, Conservatorio y Cine-debate presenciales.
			Tribunal Electoral Infantil.
			Conversatorios, Observatorios y Escuchatorios Virtual.
			Concurso de Oratoria.
			Concurso de Cortometraje.
			Congresos/Encuentros Nacionales/Regionales de Magistradas y Magistrados Electorales.
17	Dirección General de Sistemas	2	Servicio de apoyo a usuarios de equipos de cómputo.
			FIREL.
18	Dirección General de Transparencia,	4	Atención a solicitudes de acceso a la información.

ÁREA ADMINISTRATIVA		NO. INVENTARIOS ENTREGADOS	NOMBRE DEL TRATAMIENTO
	Acceso a la Información y Protección de Datos Personales		Atención a solicitudes de derechos ARCO.
			Capacitación y eventos en materia de transparencia, acceso a la información, datos personales, archivos y temas relacionados.
			Concursos en materia de transparencia, justicia abierta, acceso a la información, datos personales, archivos y temas relacionados.
19	Escuela Judicial Electoral	8	Actividades y Eventos.
			Capacitación Administrativa.
			Capacitación Externa.
			Capacitación Interna.
			Carrera Judicial.
			Formación de Posgrado.
			Acciones de formación de Posgrado con la Universidad de Girona
			Concursos Relativos a la divulgación de la materia Político Electoral.
20	Visitaduría Judicial del TEPJF	1	Visitas Ordinarias de Inspección.
21	Dirección General de Administración Regional	6	Registro de Accesos (personal y vehicular).
			Servicio médico y consentimiento.
			Circuito cerrado de televisión (CCTV).
			Adquisiciones, Arrendamientos o contratación de servicios.
			Medidas preventivas por COVID-19.
			Actividades y eventos en materia electoral.

ÁREA JURISDICCIONAL		NO. INVENTARIOS ENTREGADOS	NOMBRE DEL TRATAMIENTO
22	Secretarías Generales de Acuerdos	10	Medios de impugnación en materia electoral.
			Medios de impugnación: Juicio para la protección de los derechos político-electorales del ciudadano.
			Medios de impugnación: juicio de revisión constitucional electoral.
			Medios de impugnación: recurso de apelación, el juicio de inconformidad y el recurso de reconsideración.
			Medios de impugnación: recurso de revisión del procedimiento especial sancionador.
			Medios de impugnación: recurso de revisión.
			Conflicto o diferencia laboral entre el TEPJF y sus servidores.
			Juicio Electoral.
			Juicio para dirimir los conflictos o diferencias laborales entre el INE y sus servidores.
			Procedimiento Especial Sancionador.

V. FUNCIONES Y OBLIGACIONES DEL PERSONAL QUE TRATE DATOS PERSONALES

Para garantizar que los datos personales sean tratados de forma adecuada y con apego a las medidas y procedimientos contemplados en este documento, es necesario que las funciones y obligaciones de quienes tratan los datos personales estén claramente identificadas[3] y consten en el documento de seguridad[4].

En este sentido y de conformidad con el artículo 57 de los Lineamientos Generales de Datos, el responsable, en este caso el TEPJF, deberá establecer y documentar los roles

[3] Artículo 33, fracción II, de la Ley General de Datos.
[4] Artículo 35, fracción II, de la Ley General de Datos.

específicos de todas las personas que realicen algún tratamiento de datos personales, de conformidad con el sistema de gestión implementado.

> ***Funciones y obligaciones***
> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.*

Por ello, este TEPJF establece las obligaciones y funciones en dos niveles: de manera específica y de manera general, como a continuación se explica:

1. De forma específica, cada inventario de datos personales sometidos a tratamiento contempla un apartado exclusivo para que de manera precisa se indiquen las servidoras públicas y los servidores públicos que realizan el tratamiento, su área de adscripción y cuál es el tratamiento específico que realizan.

SERVIDORES PÚBLICOS QUE TIENEN ACCESO A LA BASE DE DATOS	ÁREA DE ADSCRIPCIÓN	FINALIDAD DEL ACCESO
Señalar los puestos de las servidoras públicas y de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente (uno por fila).	Definir unidad administrativa o jurisdiccional a la que está adscrito el puesto	Señalar con qué fines tienen acceso las servidoras públicas y los servidores públicos antes identificados (uno por fila, según corresponda).

Para completar esta sección, el área responsable verificó que las servidoras públicas y los servidores públicos señalados cuentan con atribuciones para ello de conformidad con

sus perfiles de puesto. Esta información podrá ser consultada en el **Anexo 1**, referido en el apartado anterior.

Ahora bien, de manera general, cualquier persona que realice tratamiento de datos personales en nombre del TEPJF, deberá:

1. Verificar que el tratamiento que realice se encuentre reportado en el inventario de respectivo. De no encontrarse reportado, deberá dar aviso a su superior jerárquico y a la DGTAIPDP.

2. Verificar de forma regular que el inventario que documenta el tratamiento que realiza, así como los avisos de privacidad integrales y simplificados, se encuentren actualizados.

3. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

4. Recabar el consentimiento para el tratamiento de los datos personales cuando proceda.

5. Capacitarse de manera constante en materia de protección de datos personales.

6. En razón de su nivel jerárquico:

TIPO DE MANDOS[5]	OBLIGACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES
Mandos superiores	a) Supervisar el tratamiento realizado, así como acercarse con las unidades especializadas[6] en caso de considerar que las medidas de seguridad implementadas sean las necesarias para garantizar la integralidad de los datos personales. b) Llevar el control de alta y baja de las servidoras públicas y los servidores públicos que pueden tener acceso a los datos personales en tratamiento.

[5] Fuente: Catálogo de puestos del Tribunal Electoral del Poder Judicial de la Federación, actualizado en abril de 2020.
[6] La Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales, la Dirección General de Sistemas y la Dirección General de Protección Institucional.

Mandos medios	Coadyuvar en la actualización de registros de las servidoras públicas y los servidores públicos que realizan tratamiento; así como solicitar la cancelación de los permisos respectivos cuando una persona deje de laborar para el TEPJF.
Nivel Operativo	Conocer las medidas de seguridad que debe implementar al tratar los datos personales y verificar que medidas tomar en caso de vulnerar los datos personales.

Para que los mandos superiores puedan cumplir con la obligación de definir el nivel de seguridad que requiere implementarse en un tratamiento de datos personales, es necesario que ponderen el tipo de datos personales debido al impacto o afectación que podría generar su vulneración y el tipo de soporte en el que se encuentran dichos datos.

En este sentido, y de la información que obra en los inventarios actualizados del **Anexo 1**, se puede concluir que los datos que trata el TEPJF, se pueden clasificar, para su protección, en tres niveles acumulativos: **nivel estándar, nivel sensible y nivel especial**, atendiendo a la naturaleza de la información tratada y almacenada en los documentos, y en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información almacenada en dichos documentos.

A continuación, se detallan sus características:

a) Nivel estándar. En este nivel se agrupan los datos identificativos, entre los que se encuentran de manera enunciativa más no limitativa: datos contenidos en el acta de nacimiento, en la carta de aceptación del servicio social o en la carta de presentación expedida por la institución educativa; edad, datos laborales, audios, carrera, cédula profesional, clave de elector, clave de empleado, clave única de registro de población (CURP), correo electrónico (personal/institucional/oficial), curriculum vitae, datos académicos (grado escolar y constancia de estudios), nombre, estado civil, domicilio, teléfono y ocupación, datos de identificación, datos de la pareja, datos del dependiente económico, etc.

b) Nivel Sensible: en este apartado se consideran aquellos datos que permiten la autentificación del titular de los mismos, así como datos bancarios, contratos o pólizas, reporte de incidencias, préstamo o comodato por terceros, titular de la inversión, cuenta bancaria y otro tipo de valores, saldo insoluto, acreditación de personalidad en representación de menores de edad, adeudos/pasivos, bienes inmuebles, bienes muebles, circunstancias socioeconómicas, declaraciones tributarias, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros), fideicomisario, fideicomisos, fideicomitente, régimen matrimonial y origen étnico o racial.

c) Nivel Especial. En este rubro entran los datos personales sensibles, por ejemplo, los relativos a actividades de riesgo para la salud, adicciones, alergias, antecedentes e historial clínico, características biométricas de la palma de la mano, certificado digital de la firma electrónica certificada del poder judicial de la federación, contraseña, creencias religiosas, filosóficas o morales, datos de salud, enfermedades de los miembros de la familia, estado de salud, antecedentes e historial clínico, medicamentos, hábitos de higiene, tipo de sangre, alergias, adicciones, enfermedades familiares, actividades de riesgo para la salud, diagnóstico, firma electrónica avanzada, hábitos personales de higiene, otros datos biométricos, tipo de sangre, temperatura corporal y discapacidad.

A partir de esta clasificación de los datos, los mandos superiores pueden determinar el tipo de seguridad que requieren el sistema de gestión en específico.

TIPO DE SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	NIVEL
Información adicional al número de tarjeta bancaria	Especial
Ubicación física	Sensible
Patrimonio	Sensible
Autenticación	Sensible
Jurídicos	Sensible
Salud, creencias, opiniones políticas	Sensible
Identificación y contacto	Estándar

Eliminados: catorce renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

De la revisión realizada por cada área administrativa y jurisdiccional a las medidas de seguridad que tienen implementadas, durante este proceso de actualización fue posible advertir que, salvo algunas medidas de seguridad administrativas específicas, las áreas reportaron contar con las medidas tanto físicas generales[7] y técnicas respecto a la información contenida en soportes electrónicos, las que se describen a continuación:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted] Las medidas de seguridad y protección civil en el TEPJF se tienen establecidas al margen del artículo 218 y 219 del Reglamento Interno y vertidas en los instrumentos siguientes: Lineamientos para la Protección Institucional del TEPJF, publicados en el Diario Oficial de la Federación el 8 de agosto de 2017; y el Manual de procedimiento de la Dirección General de Protección Institucional, publicado en el Diario Oficial de la Federación el 9 de agosto de 2017.

[7] Es decir, las que aplican a las instalaciones en que se encuentra en resguardo la información y no a las que cada unidad implementa de manera interna (por ejemplo tipo de cerradura o candado, registros o seguimientos internos, etc.)

Eliminados: veintiocho renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

[redacted]

11. Adicionalmente, es importante señalar que la Dirección de Seguridad Informática

[redacted]

Eliminados: doce renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

VI. ANÁLISIS DE RIESGO

Un análisis de riesgo localiza y visualiza los recursos materiales, técnicos y humanos relacionados con el tratamiento de datos personales, que están más expuestos a sufrir un daño por algún impacto negativo, para posteriormente tomar acciones o medidas adecuadas para superar las vulnerabilidades y/o amenazas.

En el análisis, se consideran aspectos como el ciclo de vida de los propios datos personales (obtención, uso, almacenamiento, transferencia, eliminación y archivo). Es decir, a través de este análisis se determinan las características del riesgo que mayor impacto podrían tener sobre los datos personales que se tratan, tomando en cuenta las amenazas y vulnerabilidades existentes que afectan la integridad, confidencialidad y disponibilidad de los datos y de los recursos invertidos en cada sistema de tratamiento, con el fin de que se prioricen y adopten los controles y/o medidas de seguridad más relevantes e inmediatos a implementar. Y, por otra parte, definir cuál es el riesgo residual, es decir, el riesgo que el responsable, el TEPJF, puede aceptar.

Una adecuada gestión de riesgo, integra la identificación, la evaluación y el control del riesgo de los activos o recursos, así como, la elaboración de evaluaciones de impacto en la protección de datos personales, cuando las áreas administrativas y jurisdiccionales consideren que concurre alguna de las condiciones previstas en el artículo 8 del Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales del Sistema Nacional de Transparencia[8].

[8] Artículo 8. Para efectos de las presentes disposiciones administrativas y en términos de lo dispuesto en el artículo 75 de la Ley General, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurra alguna las siguientes condiciones:
I. Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;
II. Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General o los que correspondan en las legislaciones estatales en la materia, entendidos como aquellos que se refieran a

Es decir, la gestión de riesgos integra: el análisis para identificar el riesgo prioritario, la elaboración de evaluaciones, la identificación las medidas correctivas, el plan de trabajo para implementarlas y el mecanismo para revisar tanto la implementación como la efectividad de las medidas.

Se trata de un análisis de riesgo que al tomar en cuenta la constante evolución tecnológica y, por lo tanto, la transformación digital que sufren los tratamientos de datos personales hace necesario que se adopte una actitud dinámica, enfocada a la gestión de los riesgos potenciales.

De forma general, el riesgo atiende a la combinación de la probabilidad de que por una vulneración ocurra una amenaza y de sus consecuencias desfavorables; de modo tal que, al determinar el riesgo en el escenario de la organización del TEPJF, se podrá realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

En este orden de ideas, durante el análisis de riesgos se realizó la revisión de todos los tratamientos de datos personales con la principal finalidad de asegurar el establecimiento de las medidas de seguridad adecuadas que garanticen el derecho a la protección de los datos personales.

Hay que destacar que para evaluar un riego fue necesario considerar todos los posibles escenarios en los que se haría efectivo, incluidos aquellos que implicaran un mal uso o abuso de los datos y las alteraciones técnicas o del entorno.

---

la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, y III. Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General o los que correspondan en las legislaciones estatales en la materia, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa mas no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

Fundamento del Análisis de Riesgos

El análisis de riesgo tiene fundamento en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos; 33, fracción IV, y 35, fracción III, de la Ley General de Datos; así como 59 y 60 de los Lineamientos Generales de Datos.

Bajo este marco normativo, el análisis de riesgos de los datos personales tratados considera lo siguiente:

- Los requerimientos regulatorios, mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- Los factores a los que se refiere el artículo 32 de la Ley General de Datos.

Metodología para el análisis de riesgos

La seguridad de los datos personales se basa en el entendimiento de la naturaleza del riesgo al que están expuestos. En algún caso, el riesgo no se podrá erradicar completamente, pero sí minimizar a través de la mejora continua.

De manera general, el riesgo atiende a la combinación de la probabilidad de que una vulneración ocurra y las consecuencias desfavorables que genere, de modo tal que, al determinar el riesgo en el escenario de la organización del TEPJF, se puede evaluar el impacto y así realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Riesgo= Probabilidad de Amenaza x Magnitud de Daño

En este contexto, los elementos para analizar los riesgos de los recursos involucrados en el tratamiento de datos personales fueron:

1. Identificación de activos de apoyo.

Un activo es un recurso (ya sea material o físico, como documentos, servicios, prácticas, políticas, instalaciones; técnico como *software* o *hardware*, o humano como personas, etc.) que tiene valor para la organización del TEPJF y necesite por tanto, ser protegido de potenciales riesgos. Los activos evaluados fueron aquéllos que se encontraban relacionados con el ciclo de vida de los datos personales previamente identificados y sus distintos tratamientos. Éstos se revisaron con el suficiente nivel de detalle para proveer la información que permitió hacer la valoración del riesgo.

De acuerdo con el artículo 59 de los Lineamientos Generales de Datos se pueden identificar tres tipos de activos de apoyo:

Técnicos:

- *Hardware* (equipo de procesamiento de datos como computadoras, servidores, equipo móvil, periféricos).
- *Software* (sistemas operativos como CPU, memoria, discos, procesos, aplicaciones, sistemas de servicio como antivirus, paquetería de software, administradores de bases de datos, mensajería instantánea, servidores web).
- Redes y Telecomunicaciones (medios y equipos).
- Soportes electrónicos (discos ópticos como CD'S y DVD'S, cintas de audio, videos y datos, discos duros removibles, memorias USB).

Material:

- Papel escrito a mano o impreso, transparencias, fotografías, expedientes, documentos.
- Infraestructura adicional (edificios, coches, instalaciones, etc.).
- Estructura organizacional (políticas, servicios, prácticas).

Eliminados: veinte renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

Humano:

- Personal (servidoras públicas y servidores públicos adscritos al TEPJF, transferentes y receptores, encargados, titulares, contratistas, terceros).

[redacted]

- [redacted]

[redacted]

2. Identificación de amenaza

Para que algo pueda ser considerado amenaza, tiene que tener el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, accidentales o deliberadas y provenir de adentro o de fuera del TEPJF.

Las amenazas se identificaron considerando que algunas pudiesen afectar a más de un activo al mismo tiempo.

Las personas responsables de los activos y sus usuarios pueden solicitar asesoría para identificar y estimar las amenazas relacionadas. Los aspectos culturales también fueron considerados dentro de las amenazas, entre otras:

AMENAZAS A LOS ACTIVOS	
Fuego	Alteración de hardware
Agua	Alteración de software
Contaminación	Rastreo de localización
Accidentes	Fallas del equipo
Polvo, corrosión, humedad, congelamiento	Malfuncionamiento del equipo
Fenómenos climáticos o meteorológicos	Saturación de los sistemas de información
Fenómenos sísmicos	Malfuncionamiento del software
Fenómenos volcánicos	Falla en el mantenimiento del sistema de información
Falla en el sistema de aire acondicionado o suministro de agua	Uso no autorizado de equipo
Pérdida de suministro eléctrico	Uso de software copiado o falsificado
Falla en los equipos de telecomunicaciones	Corrupción de datos
Intercepción e interferencia de señales	Procesamiento ilegal de los datos
Espionaje remoto	Error de uso
Escucha en comunicaciones	Abuso de privilegios
Robo de medios o documentos	Falsificación de privilegios
Robo de equipo	Denegación de acciones
Recuperación de medios desechados o reciclados	Indisponibilidad del personal
Revelación	Fecha de capacitación
Fuentes poco confiables para la obtención de datos	Extorsión

3. Probabilidad de que ocurra una amenaza

No todas las amenazas tienen la misma posibilidad de que ocurran, debido a que habrá algunas que su presencia sea remota y otras que la probabilidad pueda ser alta. Por cada amenaza, el área administrativa o jurisdiccional, con base en su experiencia y conocimiento de los activos, debe dar aviso en aquellos casos que considere que hubo alguna variación en la probabilidad de que ocurra una amenaza para que la área especializada que corresponda[9] determine si efectivamente el riesgo varió.

4. Conocimiento de vulnerabilidades por activo

La vulnerabilidad es la capacidad, las condiciones y características propias de los activos, que lo hacen susceptible a amenazas, con el resultado de sufrir un daño. Una vulnerabilidad es una debilidad en el funcionamiento o seguridad del activo y pueden ser identificadas en los siguientes ámbitos:

1. Organizacionales.
2. De procesos y procedimientos.
3. De personal.
4. Del ambiente físico.
5. De la configuración de sistemas de información.
6. Del *hardware, software* o equipo de comunicación.
7. De la relación con prestadores de servicios.
8. De la relación con terceros.

La presencia de vulnerabilidades por sí misma no causa daño, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien cuando surja algún cambio.

[9] Dirección General de Sistemas o Dirección de Protección Institucional.

Por su parte, las medidas de seguridad usadas incorrectamente o con una mala implementación son una causa de vulnerabilidad. Una medida puede ser efectiva o no, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que a su vez pueden ser usadas para propósitos distintos a los que se habían destinado originalmente[10].

En este sentido, en un primer ejercicio, respecto a vulnerabilidades atinentes a procesos, organización, procedimientos y a fin de complementar el análisis de riesgos, fue necesaria una revisión de las prácticas, actividades, servicios, procedimientos o políticas que se utilizan en cada sistema de tratamiento, a fin de advertir en éstos, aspectos que pudieran comprometer la privacidad o protección (confidencialidad, disponibilidad y/o integridad) de los datos personales involucrados.

5. Estimado del impacto a los activos a través de la identificación del posible daño (evaluación del riesgo)

El riesgo se evaluó contemplando dos elementos básicos: el primero fue el estimado del impacto negativo, bajo, medio o alto, a los activos; y el segundo fue la identificación del posible daño. Se determinó el daño que el riesgo pudiera causar a los activos, si era tolerable o debía mitigarse. Al respecto, el artículo 38 de la Ley General de Datos contempla los siguientes supuestos de vulneración:

- Pérdida o destrucción no autorizada.
- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.

[10] Deben considerarse vulnerabilidades y amenazas provenientes de diferentes fuentes, por ejemplo, la posibilidad de que un correo electrónico sea interceptado por un atacante o que un empleado envíe información confidencial a su cuenta personal.

Eliminados: diez renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

En la elaboración del análisis de riesgo fue crucial conocer el valor o relevancia de los datos personales, así como de los activos involucrados en su tratamiento para establecer en orden de prioridad la atención a los riesgos que se identificaron.

6. Revisión de prácticas relativas al tratamiento de datos

Para este apartado se realizó, a finales de 2019, la revisión de procedimientos administrativos específicos correspondientes a las direcciones generales de Asuntos Jurídicos, de Recursos Humanos y de Sistemas [redacted]

Por lo que el análisis de riesgos reportado por las direcciones generales de Sistemas y de Protección Institucional y que se adjunta como **Anexo 2,** incorpora el desglose e identificación que se realizaron sobre los riesgos que se presentan en el tratamiento de datos personales las áreas respecto de los parámetros generales para soportes físicos y electrónicos. Dichos anexos pueden ser objeto de ajuste o precisión en función del registro de vulnerabilidades que se lleguen a presentar en áreas específicas.

Eliminados: tres renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

VII.ANÁLISIS DE BRECHA

El análisis de brecha, en términos de los artículos 33, fracción V, y 35, fracción IV, de la Ley General de Datos; así como el 61 de los Lineamientos Generales de Datos consiste en identificar soluciones para reducir, mitigar o aceptar el riesgo, y, por tanto, garantizar una protección integral de los datos personales. Es decir, se trata de una herramienta que permite conocer el estado actual de las medidas de seguridad: si son suficientes para solucionar el riesgo identificado, o bien se requiere implementar otra medida.

En este sentido, la identificación de la brecha permite precisamente identificar los alcances para obtener la solución. Una vez identificada la solución, es necesario planear cómo y con qué se va a cerrar esa brecha para lograr el objetivo.

Para ello, una vez que se contó con la retroalimentación de las medidas de seguridad implementadas por las diversas áreas administrativas y jurisdiccionales, el análisis de riesgo revisado y validado por las áreas que centralizan la protección física y técnica institucional y la revisión de todos los insumos realizada por la DGTAIPDP; se definieron las medidas que se encuentran pendientes de implementación para eliminar o matizar los riesgos detectados.

Es importante señalar que para este análisis se tiene claridad en cuáles son los controles (o medidas de seguridad) que ya están funcionando de manera efectiva, así como las medidas identificadas como faltantes, para construir un programa de trabajo que refleje las expectativas a lograr, las áreas administrativas involucradas y las fechas compromiso para su implementación.

En ese contexto, [redacted]

Eliminados: veinte renglones. Fundamento legal: artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y numeral vigésimo sexto, primer párrafo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, al tratarse de información cuya publicación obstruye la prevención de los delitos (INFORMACIÓN RESERVADA). Fecha de clasificación: 7 de mayo de 2021, Décima Tercera Sesión Extraordinaria del Comité de Transparencia y Acceso a la información. Área que propuso la clasificación: Dirección de Datos Personales. Periodo de reserva: 5 años.

PLAN DE TRABAJO

Para reducir la brecha detectada e implementar las propuestas referidas, se propone el siguiente plan de trabajo:

TIPO DE MEDIDA DE SEGURIDAD QUE ATIENDE	RECOMENDACIÓN	ÁREAS INVOLUCRADAS	EXPECTATIVA	FECHA
Administrativa	Revisión de manuales de procedimientos donde se verifique que los datos personales tratados en sus procesos son estrictamente los necesarios y se implementan las medidas necesarias para garantizar los deberes de información y confidencialidad.	DGPEI y áreas que realizan tratamiento de datos personales.	• Acercamiento de la DGTAIPDP con la Dirección General de Planeación y Evaluación Institucional para explicar la relevancia de que una área realice algún proceso de actualización y manuales de procedimientos se verifique si existe tratamiento de datos y si se está contemplando la protección dentro del manual de procedimiento.	Diciembre 2020.

TIPO DE MEDIDA DE SEGURIDAD QUE ATIENDE	RECOMENDACIÓN	ÁREAS INVOLUCRADAS	EXPECTATIVA	FECHA
			• Acercamiento de la DGTAIPDP con las áreas que realizan tratamiento de datos personales para que verifiquen sus manuales de procedimientos a fin de garantizar que desde el diseño se garantice el deber de informar y de confidencialidad.	Enero 2021.
Administrativa	Implementación de procedimientos de borrado o destrucción segura de datos personales en documentos de trabajo.	Áreas que realizan tratamiento de datos personales.	Acercamiento de la DGTAIPDP con las áreas que realizan tratamiento de datos personales a fin de hacer recomendaciones para borrado o destrucción segura de datos personales en documentos de trabajo.	Diciembre 2020.
Administrativa	Elaboración de una “guía” o “decálogo” del tratamiento de datos personales, para sensibilizar, concientizar y evitar que se comentan vulneraciones por descuido y/o desconocimiento del personal operativo.	DGTAIPDP.	Elaboración y difusión electrónica de una “guía” o “decálogo” del tratamiento de datos personales, para sensibilizar, concientizar y evitar que se comentan vulneraciones por descuido y/o desconocimiento del personal operativo.	Mayo 2021.
Administrativa	Implementación de un programa de capacitación	DGTAIPDP.	Elaboración del Programa Anual de Capacitación en materia de datos personales.	Diciembre 2020.

TIPO DE MEDIDA DE SEGURIDAD QUE ATIENDE	RECOMENDACIÓN	ÁREAS INVOLUCRADAS	EXPECTATIVA	FECHA
	en materia de datos personales.		Implementación del Programa Anual de Capacitación en materia de datos personales.	Enero a Diciembre 2021.
Física.	Mejorar el mantenimiento de los archiveros, cerraduras y candados. En los casos en que los documentos se encuentren en carpetas o libreros, implementar medidas para garantizar que el acceso a ellos sea restringido.	Áreas que realizan tratamiento de datos personales.	Acercamiento de la DGTAIPDP con los enlaces de las áreas que realizan tratamiento de datos personales y que de acuerdo con las medidas reportadas encuadran en este supuesto.	Diciembre 2020.
			Implementación de medidas por parte de las áreas que tratan datos personales de implementar mejoras para garantizar el acceso restringido a los documentos.	Diciembre 2021
Técnicas.	Difusión de nuevas políticas Dirección General de Sistemas.	Dirección General de Sistemas.	Envío de las políticas aprobadas a los titulares de las unidades administrativas para su difusión.	3 meses posteriores a su aprobación.
Técnicas.	Implementar revisiones o monitoreos periódicos de la información.	Áreas administrativas que tratan datos personales.	Acercamiento de la DGTAIPDP para orientar sobre la importancia de realizar revisiones periódicas a los resguardos de información a fin de verificar que la información no haya sido vulnerada.	Abril 2021.
Técnicas.	Implementar revisiones semestrales que permitan al área responsable del	Áreas administrativas que	Acercamiento de la DGTAIPDP para orientar sobre la importancia de realizar revisiones periódicas a	Abril 2021.

TIPO DE MEDIDA DE SEGURIDAD QUE ATIENDE	RECOMENDACIÓN	ÁREAS INVOLUCRADAS	EXPECTATIVA	FECHA
	tratamiento verificar que los perfiles con acceso a los datos personales sigan estando autorizados y respeten los roles asignados.	tratan datos personales.	los perfiles autorizados para el tratamiento de datos personales, a fin de garantizar que sólo las personas autorizadas tengan acceso.	

VIII. PROGRAMA GENERAL DE CAPACITACIÓN

En seguimiento a los trabajos que año con año, realizan el TEPJF respecto a las capacitaciones en materia de transparencia, acceso a la información, datos personales y archivos y en cumplimiento con lo establecido en el artículo 33, fracción VIII, de la Ley General de Datos señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, así como lo señalado en el artículo 64 de los Lineamientos Generales de Datos que señalan:

> ***Capacitación***
> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*
>
> *En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:*
>
> ***I.*** *Los requerimientos y actualizaciones del sistema de gestión;*
>
> ***II.*** *La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
>
> ***III.*** *Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
>
> ***IV.*** *Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.*

Por lo que en cumplimiento con la Ley General de Datos, la DGTAIPDP deberá elaborar el Programa Anual de Capacitación en materia de Datos Personales con el objeto de cubrir las metas siguientes:

a) Corto Plazo 2020-2021

Sensibilización del personal que integra el TEPJF. Para esta meta se prevé proporcionar una introducción al marco teórico y legal en el tema y proporcionar ejemplos e insumos que le permitan a la servidora pública y al servidor público internalizar la importancia de la protección de datos personales, tanto en el rol de servidora pública o servidor público como el de titular de área; así como identificar hábitos que ponen en riesgo la protección de datos personales.

b) Mediano plazo 2021-2022

Formación en protección de datos personales. Para esta meta se impartirán cursos o talleres que permitan a las servidoras públicas y a los servidores públicos identificar los procedimientos a seguir en la atención de solicitudes de derechos ARCO, la actualización de avisos de privacidad e inventarios de tratamiento y para la revisión y actualización de medidas de seguridad para reducir los riesgos de vulneración de datos personales.

c) Largo plazo 2023-2026

Fortalecimiento de la protección de datos personales. Para esta meta se impartirán cursos y pláticas que permitan consolidar al interior del TEPJF la protección de datos personales como una actividad intrínseca a sus funciones.

El Programa Anual de Capacitación en materia de Datos Personales deberá ser presentado a más tardar en la última sesión ordinaria de cada año del Comité de Transparencia, y deberá diseñarse de tal forma que permita el cumplimiento de las metas señaladas, así como de las necesidades específicas que se detecten durante su implementación.

IX. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El artículo 36 de la Ley General de Datos establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, cuando se actualice alguno de los supuestos antes citados, la DGTAIPDP lo hará del conocimiento del Comité de Transparencia con el objeto de que este determine si considera procedente la actualización del presente documento de seguridad.

Todos los sistemas de tratamiento que integran el documento de seguridad del TEPJF deben mantenerse actualizados; sin embargo, se entenderá que las modificaciones implican la necesidad de actualizar el documento de seguridad cuando al adecuarse el nivel de riesgo reportado las medidas de seguridad resulten insuficientes.

Aprobación del Documento de Seguridad: 18 de febrero de 2019.
Primera actualización. Fecha de aprobación: 16 de octubre de 2020.