TRIBUNAL ADMINISTRATIVO

TA

DEL PODER JUDICIAL DEL ESTADO
CHIAPAS

DOCUMENTO DE SEGURIDAD

TRIBUNAL ADMINISTRATIVO DEL PODER JUDICIAL DEL ESTADO DE CHIAPAS

Las suscritas Magistradas Susana Sarmiento López, Mónica de Jesús Trejo Velázquez y el Magistrado Víctor Marcelo Ruiz Reyna, integrantes del Pleno del Tribunal Administrativo del Poder Judicial del Estado, en ejercicio de las facultades que nos confieren los artículos 79, de la Constitución Política del Estado Libre y Soberano de Chiapas; 49 y 50 de la de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; 11, fracción XXXI de la Ley Orgánica y 9, fracciones VIII y XXII del Reglamento Interior ambos ordenamientos del Tribunal Administrativo del Poder Judicial del Estado, y en atención al siguiente:

CONSIDERANDO

Que el derecho a la protección de los datos personales se encuentra consagrado en las disposiciones 6 y 18 de la Constitución Política de los Estados Unidos Mexicanos, de dicho derecho surgen 4 vertientes principales, como lo son el derecho de acceso, rectificación, cancelación y oposición al tratamiento de los datos de mérito.

En esa tesitura, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo subsecuente Ley General de Protección) en relación con lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (en adelante Ley Estatal de Protección), son un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura el Tribunal Administrativo del Poder Judicial del Estado de Chiapas (en adelante TAPJECH y/o Tribunal Administrativo).

Que, con base en el artículo 3, fracción XIV de la Ley General de Protección, en adminiculación con el numeral 5, fracción XIII de la Ley Estatal de Protección, el Documento de Seguridad es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Documento que tiene como propósito establecer la forma de tratar los datos personales que lleva a cabo el Tribunal, por los órganos jurisdiccionales y administrativos que conforman

su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de la información confidencial, además de desarrollar buenas prácticas en la materia.

Que, con base en lo anterior, el Tribunal ha identificado los procesos que dentro de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de éstos durante el ciclo de vida de la información, indicando la manera en la que se tratan, las medidas de seguridad adoptadas y los órganos jurisdiccionales y administrativos que son responsables de su protección, así como las finalidades del tratamiento acorde a sus funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran forman parte de un sistema interno para la gestión y tratamiento de los datos personales en posesión del TAPJECH, pues tal y como lo dispone el artículo 34 de la Ley General de Protección, así como los dispositivos 48 y 49 de la Ley Estatal de Protección, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Por ende, el TAPJECH comprometido con la tutela de los datos personales que trata y en consonancia con lo establecido en la normatividad de la materia, así como las recomendaciones y cursos recibidos por el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, que han impulsado en su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

De ahí que el presente Documento de Seguridad, permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

Por los fundamentos y consideraciones anteriormente expuestas, las Magistradas y el Magistrado, integrantes del Pleno del Tribunal Administrativo del Poder Judicial del Estado, tienen a bien expedir el Documento de Seguridad en materia de protección de datos personales, acorde a lo siguiente:

INDICE

I.- Disposiciones generales

Además de las disposiciones establecidas en el numeral 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en el artículo 5 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y de acuerdo al Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales del TAPJECH, en este ordenamiento se entenderá por:

Área de Informática: a la instancia del TAPJECH, dependiente de la Unidad de Apoyo Administrativo, encargada de vigilar el cumplimiento de las normas, políticas y procedimientos que en materia de informática establezca el Pleno del Tribunal Administrativo, conforme a lo señalado en el artículo 64 del Reglamento Interior del TAPJECH.

Área de Recursos Materiales y Servicios Generales: a la instancia del TAPJECH, dependiente de la Unidad de Apoyo Administrativo, encargada de implementar las medidas de seguridad necesarias para preservar el patrimonio del Tribunal, conforme a lo señalado en el artículo 62, fracción XXIV del Reglamento Interior del TAPJECH.

Contraloría: a la instancia del TAPJECH, encargada de planear, organizar y coordinar el sistema de prevención, control y vigilancia de la administración del Tribunal, que cuenta con autonomía técnica y de gestión para cumplir cabalmente sus atribuciones, señaladas en el artículo 36 y 37 de la Ley Orgánica del TAPJECH, lo aplicable de la Ley de Responsabilidades Administrativas para el Estado de Chiapas, así como del Reglamento Interior del TAPJECH.

Grupo Interdisciplinario: al conjunto de personas que coadyuvan en el análisis de los procesos y procedimientos institucionales que dan origen a la documentación, así como en la identificación de los valores documentales, vigencias, plazos de conservación y disposición documental, durante el proceso de valoración documental del TAPJECH.

ITAIPCH y/u Órgano Garante Local: al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

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

Ley Estatal de Protección: a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

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

Oficial de Protección de Datos Personales: a la persona servidora pública que desempeña las atribuciones señaladas en el artículo 75 Bis del Reglamento Interior del TAPJECH, con adscripción a la Unidad de Transparencia.

Órganos jurisdiccionales: al Juzgado de Jurisdicción Administrativa, Juzgado Especializado en Responsabilidad Administrativa, y Sala de Revisión del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Órganos administrativos: a las áreas de carácter administrativo que auxilian en la labor sustancial del TAPJECH.

Sistema de Gestión: al presente Sistema de Gestión de Seguridad de Protección de Datos Personales del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, consistente en el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en el TAPJECH.

Titular: a la persona particular o servidora pública titular de los datos personales.

Tribunal Administrativo o TAPJECH: al Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Unidad de Transparencia: a la Unidad de Transparencia del TAPJECH.

Unidad de Apoyo Administrativo: al órgano administrativo encargado de administrar y controlar el presupuesto de egresos autorizado para cada ejercicio, de acuerdo a la normatividad aplicable, así como para proponer medidas que tiendan a la preservación y al mejoramiento administrativo del Tribunal.

II.- Objeto y alcance del Documento de Seguridad

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado el TAPJECH para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por los órganos jurisdiccionales y/o administrativos, conforme a lo establecido en la Ley General de Protección, la Ley Estatal de Protección y en los Lineamientos Generales de Protección.

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de la Sala de Revisión (a través de la Secretaría General de Acuerdos y del Pleno), la Presidencia (a través de personal designado), los Juzgados de Jurisdicción Administrativa, y Especializado en Responsabilidad Administrativa, la Contraloría, la Unidad de Apoyo Administrativo con las áreas que la componen como lo son: Recursos Humanos, Recursos Materiales y Servicios Generales, Recursos Financieros, Informática, y Planeación, así como las Áreas de Comunicación Social, Defensoría de Oficio, Coordinadora de Archivos, y la Unidad de Transparencia, en las que, de acuerdo con su ámbito de funciones, se llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad, tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan los datos personales.

En este sentido, la Unidad de Transparencia integra el presente Documento de seguridad con base en la información generada por los órganos

jurisdiccionales y administrativos citadas en antelación, acorde al ámbito de sus funciones y de conformidad con las disposiciones jurídicas aplicables.

No es óbice señalar que, en el ámbito de sus respectivas competencias y bajo el marco normativo aplicable en la materia, las disposiciones expuestas en este documento resultan de observancia obligatoria para los órganos jurisdiccionales y administrativos que realicen tratamientos de datos personales.

En atención a ello, se hace saber a las personas servidoras públicas del TAPJECH que la Unidad de Transparencia se encuentra a su disposición para brindar la orientación necesaria en relación con el presente documento, la cual podrá solicitarse:

Vía correo electrónico: atransparencia@tachiapas.gob.mx y/o tapje.transparencia@gmail.com

Vía telefónica: 9613469030, ext. 2517.

Vía presencial: en la Unidad de Transparencia ubicada en el piso 4, del edificio con dirección en avenida 16 poniente Sur, 1713, Colonia Xamaipak, Ciudad de Tuxtla Gutiérrez, Chiapas, código postal 29067.

III.- Relevancia y base del Documento: Deber de Seguridad

El artículo 31 de la Ley General de Protección, en relación con el dispositivo 45 de la Ley Estatal de Protección, establece que, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el TAPJECH tendrá 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, destrucción o uso, acceso o tratamiento no autorizado.

- Garantizar su confidencialidad, integridad y disponibilidad.

En ese sentido, los artículos 3, fracciones XIV, XX, XXI, XXII y XXIII y 35 de la Ley General de Protección; 4, fracciones XIII, XXIV, XXV, XXVI y XXVII, 49 y 50 de la Ley Estatal de Protección, disponen la descripción de manera particular de dichas medidas a través de la elaboración de un Documento de Seguridad.

De modo que, en acatamiento del deber de seguridad de los datos personales, en todos los sistemas en que se efectúe un tratamiento de datos personales, el TAPJECH (a través de las instancias responsables) debe realizar lo siguiente:

Proteger los datos personales contra un probable daño, pérdida, alteración, destrucción, o uso, acceso o tratamiento no autorizado.

A través de medidas de seguridad administrativas, físicas y técnicas.

Las cuales deben de constar en un documento de seguridad.

Lo anterior, conservando su confidencialidad, integridad y disponibilidad.

IV.- Medidas de Seguridad de los Datos Personales del TAPJECH

Para el tratamiento de los datos personales que lleva a cabo el TAPJECH a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su seguridad, confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección, en relación con lo dispuesto en la Ley Estatal de Protección, y lo contemplado en los Lineamientos Generales de Protección.

En tal virtud, el TAPJECH dio inicio a la planificación de los esquemas de protección de datos personales mediante la identificación de todos y cada uno de los procesos y tareas de acuerdo con el ámbito de funciones de las distintas áreas que conforman la estructura jurisdiccional y administrativa de este Organismo Colegiado Judicial.

De tal método se previeron acciones para optimizar y precisar el modo de levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases (físicas o electrónicas de datos); las finalidades del tratamiento, y, si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Hasta este punto, la norma general jurídica-administrativa que funge como eje rector en el actuar de las personas titulares de los órganos jurisdiccionales y administrativos del TAPJECH, lo es la Ley Orgánica del TAPJECH, pues dispone que este Órgano Colegiado es la máxima autoridad jurisdiccional en materia administrativa, que forma parte del Sistema Anticorrupción del Estado de Chiapas, resolviendo con base en los principios de legalidad, máxima publicidad, respeto a los derechos humanos, verdad material, razonabilidad, proporcionalidad, presunción de inocencia, tipicidad y debido proceso.

En su actuar, el personal jurisdiccional y administrativo, que formen parte del quehacer institucional del TAPJECH, en el ámbito de sus respectivas competencias y en el ejercicio de sus funciones, se encuentran obligados a promover, respetar, proteger y garantizar los derechos humanos, de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad, y prestando su servicio bajo los principios de excelencia, objetividad, imparcialidad, independencia y profesionalismo, tomando en cuenta de manera ininterrumpida, sin distinción ni excepción, conforme a sus funciones y responsabilidades respectivas, en toda relación institucional, su actuación guiada por los Principios Constitucionales y Legales rectores que rigen al Servicio Público y Valores Institucionales, establecidos en el Código de Ética del TAPJECH.

En ese contexto, la responsabilidad de cada tratamiento a los datos personales que se desarrollan en cada instancia (órgano jurisdiccional y/o administrativo) del TAPJECH, recae en cada persona titular de éstas, en virtud de estar en vías de instaurar e identificar a los datos como: el nombre,

cargo y adscripción, de las personas servidoras públicas que tienen acceso a la operación sobre esa información.

Sin embargo, dentro del proceso primigenio de implementación sobre la designación oficial del inventario general de tratamientos, ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que las personas servidoras públicas del TAPJECH que intervienen en el tratamiento conocen a través de las disposiciones que la Ley General de Protección, en relación con la Ley Estatal de Protección que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que los órganos jurisdiccionales y administrativos, realizan conforme a las disposiciones que regulan la gestión documental al interior de la institución.

De igual forma, una vez integrados los inventarios de datos, se dispuso de una metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV de la Ley General de Protección, en relación con el numeral 47, fracción IV de la Ley Estatal de Protección, los órganos jurisdiccionales y administrativos del TAPJECH responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para las titulares de los mismos con motivo de su posible vulneración y los factores de riesgo a los que eventualmente se encuentran expuestos.

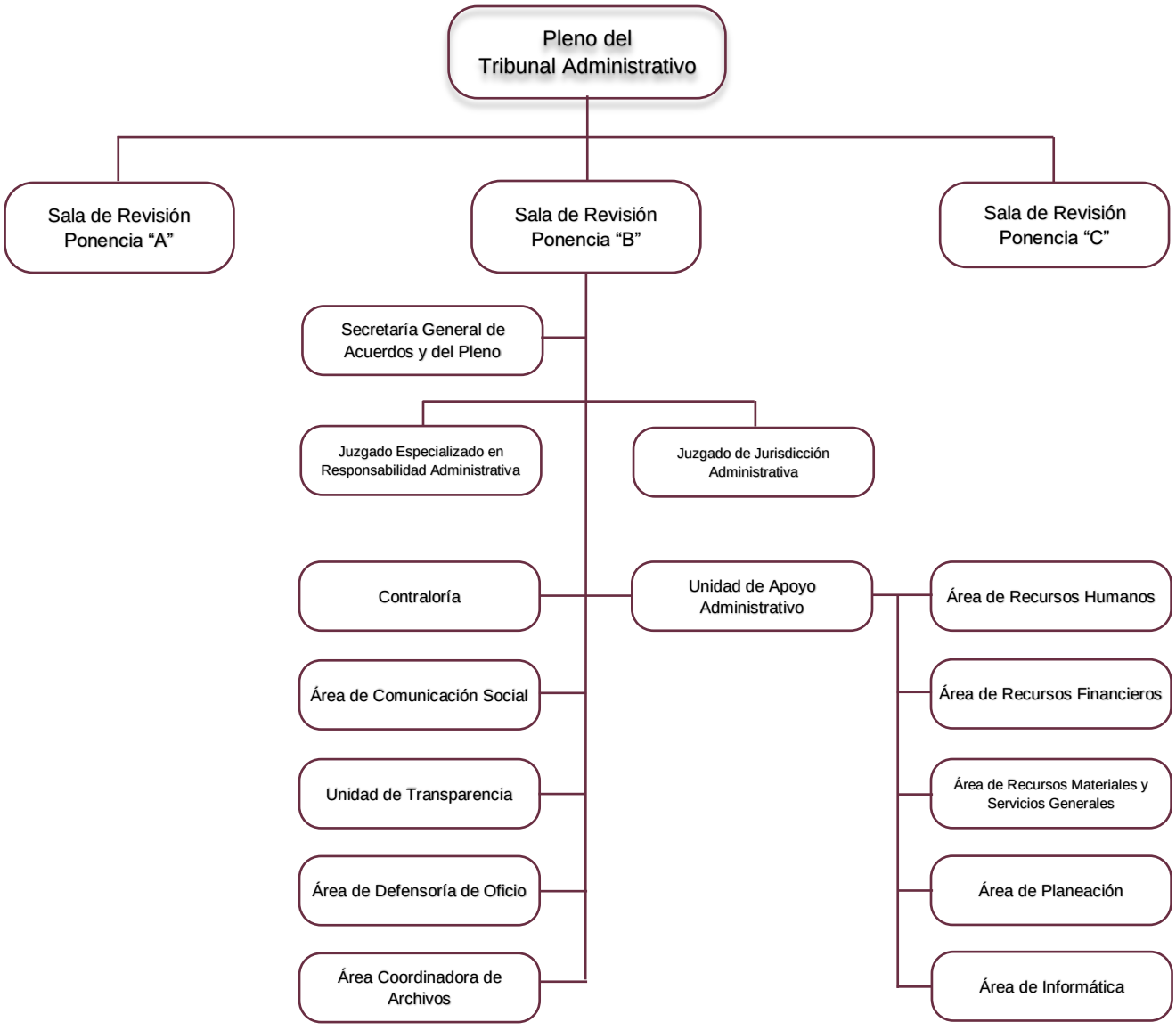
Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad **administrativas**, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información, también están las **físicas**, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento, además de las **técnicas** que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de

brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados.

En ese tenor, las medidas de seguridad generales del TAPJECH se clasifican conforme a lo siguiente:

1. Administrativas:

1. Estructura orgánica y organigrama general de las unidades/áreas administrativas del TAPJECH.[1]



[1] Disponible en el Manual de Inducción del Tribunal Administrativo del Poder Judicial del Estado de Chiapas página 7, conforme a la Opinión Técnica número: SH/CGRH/DEO/0057/2022.

2. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

3. Mecanismos de control para el cumplimiento de los principios y deberes en materia de protección de datos personales establecidos en el Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales del TAPJECH.

2. Físicas:

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.

2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.

3. Limitar el número de personas con acceso a archivos físicos.

4. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

5. Las estipuladas por las personas servidoras públicas en ejercicio de las facultades y responsabilidades inherentes a su cargo, entre las que se destacan:

    - Almacenamiento bajo llave de los datos personales documentados en papel.

    - El acceso a los datos personales condicionado al personal autorizado.

3. Técnicas:

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata al Área de Informática de la Unidad de Apoyo Administrativo, los casos en los que las personas servidoras públicas identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. No dejar documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado, si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que no sean necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

11. Las estipuladas por las personas servidoras públicas en ejercicio de las facultades y responsabilidades inherentes a su cargo, entre las que se destacan:

    - Condicionar el acceso a los datos personales al personal autorizado.
    - Que las personas servidoras públicas con acceso autorizado, cuenten con contraseña particular.
    - Que la contraseña sea única para el acceso a los datos personales.

Relativo a los buenos hábitos internos que debe realizar cada órgano jurisdiccional y administrativo; se tomará a consideración lo siguiente:

1. Mantener el área de trabajo sin documentos importantes y/o dispositivos de almacenamiento electrónico a la vista.

2. Cerrar los cajones y resguardar la información personal bajo su custodia.

3. Evitar dejar los documentos que ya no sean utilizados sobre escritorios, impresoras, escáneres o copiadoras.

4. Realizar la eliminación segura de información en equipos de cómputo, tabletas y medios de almacenamiento electrónico.

5. Realizar respaldos periódicos de los datos personales.

6. Utilizar cerraduras y candados en espacios donde se resguarda información que contiene datos personales.

7. Bloquear o suspender la sesión en equipos de cómputo cuando se dejen de utilizar.

8. Validar el destinatario antes de realizar una remisión o transferencia de la información.

A manera de implementar mejores prácticas, y de conformidad con lo establecido en los artículos 30, fracción II, 72, 84, fracciones I y V, 85, fracción III, y segundo párrafo de la Ley General de Protección, en relación con los dispositivos 44, fracción II, 100, 110, fracción II, 113, 114, fracciones I y VI, y 117, fracciones III y VIII de la Ley Estatal de Protección, el Comité de Transparencia del TAPJECH dispone las siguientes medidas:

1. Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General de Protección, en relación con lo dispuesto en la Ley Estatal de Protección, estrictamente para propósitos legales o legítimos del TAPJECH;

2. Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Leyes citadas;

3. Informar a las titulares del tratamiento de los datos personales y sus finalidades;

4. Procurar que los datos personales tratados sean correctos y estén actualizados;

5. Suprimir los datos personales cuando hayan dejado de ser necesarios de acuerdo a las finalidades para las cuales se obtuvieron;

6. Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;

7. No obtener datos personales a través de medios fraudulentos;

8. Respetar la expectativa razonable de privacidad de la titular;

9. Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

10. Velar por el cumplimiento de los principios;

11. Establecer y mantener medidas de seguridad;

12. Guardar la confidencialidad de los datos personales;

13. Identificar el flujo y ciclo de vida de los datos personales;

14. Mantener actualizado el inventario de datos personales o de las categorías que maneja el TAPJECH;

15. Respetar los derechos de las titulares en relación con sus datos personales;

16. Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y

17. Identificar a las personas servidoras públicas del TAPJECH responsables del tratamiento de los datos personales.

V.- De las Vulnerabilidades

1. Se consideran posibles vulnerabilidades a la seguridad, dentro de las etapas de los tratamientos a datos personales en posesión del TAPJECH, las siguientes:

a) Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.

b) Deficiente conocimiento de procedimientos en materia de seguridad de datos.

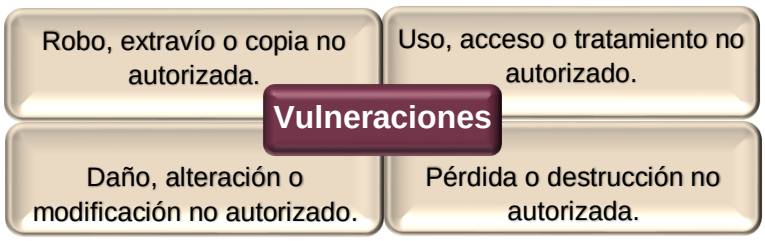
c) Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).

d) Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.

e) Falta de seguimiento y monitoreo a políticas de seguridad.

f) Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

2. Por otra parte, de conformidad con lo establecido en el dispositivo 38 de la Ley General de Protección, en relación con el diverso 52 de la Ley Estatal de Protección, se consideran vulneraciones de seguridad, en cualquier etapa de tratamiento de datos personales, las siguientes:



VI.- Inventario de Tratamientos y de Datos Personales del TAPJECH

Conforme a los artículos 33, fracción III, y 35, fracción I, de la Ley General de Protección, en adminiculación con los dispositivos 47, fracción III, y 50, fracciones I, II, III, IV y V de la Ley Estatal de Protección, y tomando en consideración las definiciones de fuente de acceso público inherentes al tema, en fomento al uso de las tecnologías para garantizar la transparencia, el derecho de acceso a la información pública y la protección de datos personales, así como promover la generación, documentación y publicación de instrumentos a través de formatos abiertos y accesibles, el Inventario de Tratamientos y de Datos Personales del TAPJECH (anexo no. 1), podrá visualizarse a través del apartado de Protección de Datos Personales en la página web institucional del TAPJECH, mismo que forma parte del presente Documento de Seguridad.

Para pronta referencia, se facilita el contexto general de los tratamientos a datos personales, según los órganos jurisdiccionales y/o administrativos, mediante el cuadro siguiente:

No.	ORGANO JURISDICCIONAL y/o UNIDAD/ÁREA ADMINISTRATIVA	NÚM. DE TRATAMIENTOS DECLARADOS	TRATAMIENTO
1	Presidencia	2	Acciones de capacitación presencial y/o virtual, dirigidas a sujetos obligados.
			Convenios de colaboración con instituciones públicas y privadas.
2	Sala de Revisión a través de la Secretaría General de Acuerdos y del Pleno	2	De los recursos de revisión derivados de los juicios contenciosos administrativos, que sean turnados a la Sala de Revisión.
			De los recursos de revisión de responsabilidad administrativa y de apelación derivados de procedimientos de responsabilidad administrativa, que sean turnados a la Sala de Revisión a través de la Secretaría General de Acuerdos y del Pleno.
3	Sala de Revisión erigido en Tribunal de Sentencia	1	Respecto a los Datos Personales contenidos en los Asuntos de Juicio Político que el Congreso del Estado presenta a la Sala de Revisión del TAPJECH.
4	Juzgado de Jurisdicción Administrativa	1	Juicios Contenciosos Administrativos.
5	Juzgado Especializado en Responsabilidad Administrativa	2	Juicios Contenciosos Administrativos.
			Procedimientos de Presuntas Responsabilidades Administrativas
6	Contraloría	3	Declaraciones de situación patrimonial y de intereses.
			Actas de entrega-recepción.

			Recepción de quejas y/o denuncias en materia de responsabilidad administrativa.
7	Área de Defensoría de Oficio	1	Prestación de Servicio en Materia de Responsabilidad Administrativa del Área de Defensoría de Oficio.
8	Unidad de Transparencia	4	Solicitudes de acceso a la información al TAPJECH.
			Solicitudes para el ejercicio de los Derechos ARCO.
			Recursos de revisión en materia de solicitudes de acceso a la información.
			Recursos de revisión en materia de datos personales.
9	Área de Comunicación Social	1	Para las personas usuarias de las plataformas digitales vinculadas con la promoción y difusión de labores institucionales.
10	Unidad de Apoyo Administrativo, en conjunto con el Área de Recursos Financieros	1	Emisión de Certificados de Depósito.
11	Área de Planeación, en conjunto con el Área de Recursos Financieros	2	Emisión de suficiencia presupuestal y pago a proveedores.
			Emisión de suficiencia presupuestal y pago de nómina.
12	Área de Informática	3	Creación de la firma electrónica.
			Elaboración de Resguardos de Bienes Informáticos.
			Cámaras de videograbación.
13		5	Procedimiento de contacto a posibles proveedores.

	Área de Recursos Materiales y Servicios Generales		Resguardo personal de mobiliario y equipo.
			Procedimiento de contratación y pago a proveedores.
			Procedimiento de contratación para la adquisición de bienes y prestación de servicios.
			Registro de entradas y salidas de las personas visitantes.
14	Área de Recursos Humanos	3	Elaboración y seguimiento de expediente personal.
			Registro de entradas y salidas de personas servidoras públicas del Tribunal, y prestadoras de servicio social y prácticas profesionales.
			Expedientes de prestadores de servicio social y prácticas profesionales.

VII.- Análisis de Riesgo y de Brecha

De conformidad con el artículo 33, fracción IV de la Ley General de Protección, en relación con el artículo 47, fracción IV de la Ley Estatal de Protección, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes para los datos personales que son recabados y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, el tipo de hardware, software o las características del responsable, entre otros.

Asimismo, para el caso del análisis de brecha, según lo establecido en el numeral 34, fracción V de la Ley General de Protección, en relación con el dispositivo 47, fracción V de la Ley Estatal de Protección, se debe realizar comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

Sin embargo, en lo que atañe a la materia de Protección de Datos Personales, la Ley General de Protección, en relación con lo que establece la Ley Estatal de Protección, éstas detallan la observancia de la Ley General de Transparencia y Acceso a la Información Pública, en adminiculación con lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, pues en dichas normativas, el ejercicio del derecho de acceso a la información pública comprende el efecto de buscar, investigar, solicitar, recibir y difundir información, así como la consulta física a los documentos, la orientación sobre su existencia y contenido conforme a los medios establecidos en ley, y bajo las restricciones de información señaladas en los *Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas,* partiendo de los preceptos de información reservada o confidencial.

En este caso, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante acuerdo publicado

en el Diario Oficial de la Federación de fecha 26 de noviembre del año 2021, aprobó los *Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,* a través de los cuales, la *Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia,* en las disposiciones de la Vertiente 2: Deberes, Variable 2.1:Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1., establecen lo siguiente:

> *"…En caso de tratarse del documento de seguridad, deberá incluir la versión pública del mismo. Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio…" (Sic)*

En tal virtud e interpretación de dicha metodología, y con el objeto de no incumplir con el Deber de Seguridad, mismo que los sujetos obligados deben observar y vigilar, los Análisis de Brecha y de Riesgo se detallan en los anexos digitales números 2.1 y 2.2 del presente Documento de Seguridad, pero su contenido oficial no se hace de conocimiento al público por los motivos anteriormente señalados.

Por otra parte, a través del apartado de Protección de Datos Personales dispuesto en la página web institucional del TAPJECH, se facilitan los formatos de los análisis de mérito, con motivo de que las personas interesadas conozcan el mecanismo para la detección de los riesgos y las brechas sobre las medidas de seguridad y categorías de datos personales de los tratamientos del TAPJECH.

VIII.- Plan de Trabajo

Con fundamento en el numeral 33, fracción VI de la Ley General de Protección, en relación con el artículo 47, fracción VII de la Ley Estatal de Protección, se advierte la obligación de establecer y mantener las medidas de seguridad, bajo el método de elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Lo anterior, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, considerando los recursos designados, el personal interno de los órganos jurisdiccionales y/o administrativo y las fechas destinadas para la implementación de las medidas de seguridad nuevas o faltantes.

De tal forma, el Plan de Trabajo se implementará de manera concentrada, como resultado de los Análisis de Brecha y de Riesgo, que en materia de seguridad de datos personales afronten los órganos jurisdiccionales y/o administrativos, conforme a las medidas de seguridad que se estiman deben implementarse, en el contexto de su propia organización interna y la evolución tecnológica de los sistemas.

No se omite precisar que, tal y como se refirió en el apartado de Análisis de Riesgo y de Brecha, no se publican las acciones definidas en el Plan de Trabajo, por las disposiciones contempladas en la *Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.*

IX.- Mecanismos de monitoreo, revisión, alertas, vulneraciones y auditoría

El artículo 30, fracción V de la Ley General de Protección, en relación con el numeral 44, fracción V de la Ley Estatal de Protección, establecen que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permitan comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, los artículos 35, fracción VI de la Ley General de Protección, y 50, fracción XVIII de la Ley Estatal de Protección, establecen que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, los numerales 33, fracción VII de la Ley General de Protección, y 47, fracción VII de la Ley Estatal de Protección, disponen que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales; y/o,

2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales.

Respecto del monitoreo y supervisión periódica de las medidas de seguridad, el artículo 63 de los Lineamientos Generales de Protección dispone que el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo anterior, dicho numeral estipula que se deberá monitorear continuamente lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos (activo es todo elemento de valor involucrado en el tratamiento de datos personales, como pueden ser una base de datos, el conocimiento de

los procesos, el personal, el hardware, el software, los archivos o los documentos en papel).

- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.
- Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Los incidentes y vulneraciones de seguridad ocurridos.

Además de lo expuesto, el artículo referido indica que el responsable deberá contar con un programa para monitorear y revisar la eficacia y eficiencia del sistema de gestión de seguridad, incluyendo auditorías para verificar el nivel del avance de las acciones en la materia, desarrolladas por los órganos jurisdiccionales y administrativos del TAPJECH.

Para ello, los órganos jurisdiccionales y/o administrativos, se auxiliarán en todo momento del Área de Informática, con efecto de emitir dictámenes, opiniones técnicas, y en su caso, los resultados de la revisión a los activos de carácter electrónico, incluyendo acciones preventivas y correctivas.

Respecto a los bienes muebles que se encuentren involucrados en el desarrollo de las acciones de auditoría, monitoreo y revisión, la Unidad de Transparencia solicitará a la Unidad de Apoyo Administrativo, con efecto de instruir al Área de Recursos Materiales y Servicios Generales, para que designe personal y auxilie en la valoración del estado físico de los bienes mencionados, conforme al artículo 62, fracciones XI, XXIV y XXXI del Reglamento Interior del TAPJECH.

En el desarrollo de los mecanismos de actuación establecidos en el presente capítulo, el Área de Informática brindará el apoyo técnico y/o tecnológico respectivo a los órganos jurisdiccionales y administrativos, conforme a la normatividad en la materia, para el cumplimiento del Sistema de Gestión.

Las áreas de Informática y Recursos Materiales y Servicios Generales, darán cuenta de sus acciones a la Unidad de Apoyo Administrativo de manera oficial con copia a la Unidad de Transparencia, con efecto de que se haga del conocimiento a la Presidencia del TAPJECH.

Asimismo, para el auxilio en el desarrollo de los mecanismos de auditoría, la Unidad de Transparencia solicitará al Área Coordinadora de Archivos, con el efecto de habilitar al personal para brindar asesoría técnica sobre operación de los archivos, observar el soporte documental (físico o electrónico) de los tratamientos de datos personales y vigilar la aplicación de instrumentos archivísticos de los órganos jurisdiccionales y administrativos, ello conforme al artículo 29, fracciones VI, XIII y XV de la Ley de Archivos del Estado de Chiapas, así como los numerales 126 y 127, fracciones II, VII y XI del Reglamento Interior del TAPJECH, lo anterior, previa autorización de la Presidencia del TAPJECH.

Así, bajo un esquema de mejora continua, a efecto de mantener el monitoreo y revisión de los aspectos en cita, se presentan los mecanismos siguientes:

A. Mecanismo de monitoreo y supervisión en la protección de datos personales.
B. Mecanismo de actuación ante alertas y vulneraciones a la seguridad de los datos personales.
C. Mecanismo de Auditoría en Materia de Datos Personales.

A. Mecanismo de monitoreo y supervisión.

Para establecer y mantener la seguridad de los datos personales, los artículos 33, fracción VII, de la Ley General de Protección, y 47, fracción VII de la Ley Estatal de Protección, establecen que se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Al respecto, la Unidad de Transparencia será la instancia encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, el cual se integrará por las etapas de monitoreo y supervisión.

La etapa de monitoreo consistirá en el requerimiento por parte de la Unidad de Transparencia, que deberá ser desahogado por los órganos jurisdiccionales y/o administrativos que, en el ámbito de sus atribuciones, sean las encargadas de los sistemas de tratamiento de datos personales.

La etapa de supervisión consistirá en el análisis por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales, al cual corresponderá un Dictamen de Seguridad de Datos Personales en el que se plasmen las recomendaciones pertinentes.

Dichos procesos, se describen gráficamente de la forma siguiente:

Etapa	Objetivo	Ejecución	Documento final
Monitoreo	Registrar los controles de seguridad instaurados en determinado tratamiento.	Los órganos jurisdiccionales y/o administrativos competentes describirán las medidas implementadas para la seguridad de los datos personales.	Reporte de Seguridad de los Datos Personales.
Supervisión	Valoración de la efectividad de los controles de seguridad instaurados.	La Unidad de Transparencia analizará el Reporte de Seguridad de los Datos Personales emitido por el órgano jurisdiccional y/o administrativo.	Dictamen de Seguridad de los Datos Personales.

A continuación, se describen cada una de las etapas citadas.

I. Etapa de Monitoreo

Se realizará tomando como punto de partida lo informado por cada órgano jurisdiccional y/o administrativo ante la Unidad de Transparencia en la integración del Documento de Seguridad, lo cual abarcará, entre otros aspectos, lo siguiente:

- Datos personales que se obtienen o reciben en cada tratamiento.
- Motivos y fundamento legal por los cuales se recaban o reciben los datos personales.
- Tecnologías empleadas para el tratamiento.
- Medidas de control implementadas, incluyendo su objetivo, la forma en que se instrumentan y el responsable de su ejecución.
- Identificación de controles preventivos.
- Identificación de controles correctivos.

En vista de lo anterior, la Unidad de Transparencia, a través de la o el Oficial de Protección de Datos Personales, requerirá a cada órgano jurisdiccional y/o administrativo, por cada uno de los tratamientos que realiza, la elaboración del Reporte de Seguridad de Datos Personales, en el que deberán precisarse los elementos siguientes:

1. Acciones desarrolladas para la ejecución de las medidas de control existentes.
2. Manifestación acerca de si existe alguna actualización o modificación respecto de las medidas de seguridad y controles implementados en el tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación.

Para la identificación respectiva de los controles implementados, los órganos jurisdiccionales y/o administrativos se auxiliarán del Área de Informática, con el fin de evitar contradicciones en la utilización y señalamiento de controles.

3. Indicar de manera clara la actualización de los aspectos siguientes:

- La incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.

- El surgimiento de nuevas amenazas en el tratamiento de los datos.

- La posibilidad de que las nuevas amenazas actualicen una vulnerabilidad en el tratamiento de datos respectivo.

- Casos en los que una amenaza haya sufrido alguna modificación que derive en el incremento del impacto que tendría su materialización en la seguridad de los datos personales.

El requerimiento a cada órgano jurisdiccional y/o administrativo del Reporte de Seguridad de Datos Personales se realizará de acuerdo con el calendario respectivo, mismo que será propuesto por la o el Oficial de Protección de Datos Personales, elaborado por la Unidad de Transparencia y sometido a consideración del Comité de Transparencia para su aprobación.

El formato del referido reporte constituye el anexo 3 de este documento.

II. Etapa de Supervisión

La o el Oficial de Protección de Datos Personales analizará los reportes de seguridad de datos personales remitidos por los órganos jurisdiccionales y/o unidades/áreas administrativas, verificando especialmente lo siguiente:

- La idoneidad y efectividad de las medidas de seguridad y control respecto al tratamiento.

- La suficiencia de controles preventivos y correctivos.

- La gestión interna de nuevas amenazas, vulnerabilidades e incrementos en el impacto de probables daños.

- El cumplimiento de políticas, planes, procesos y procedimientos en materia de seguridad de datos personales.

Posterior a su examinación, elaborará un Dictamen de Seguridad en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad.

Lo que será notificado a los órganos jurisdiccionales y/o administrativos, puntualizando las cuestiones que se estimen de atención prioritaria, señalando la forma en que las recomendaciones y/o requerimientos habrán de ser desahogados, destacando el plazo en que deberán remitirse las evidencias de su cumplimiento a la o el Oficial de Protección de Datos Personales.

Si de las recomendaciones concluidas puede derivarse una estrategia que maximice la seguridad de los datos personales, la o el Oficial de Protección de Datos Personales propondrá a la Unidad de Transparencia la actualización del presente Documento de Seguridad en el apartado correspondiente, con el objeto de que sean atendibles por aquellos órganos jurisdiccionales y/o administrativos que les pueda resultar aplicable.

Asimismo, de advertir una modificación sustancial a determinado tratamiento que derive en un cambio en su nivel de riesgo o una estrategia que maximice la seguridad de los datos personales que pueda ser aplicable a los órganos jurisdiccionales y/o administrativos, la Unidad de Transparencia deberá analizar la necesidad de actualizar el Documento de Seguridad, en términos de lo establecido para esos efectos.

El formato del referido dictamen constituye el anexo 4 de este documento.

B. Mecanismos de actuación ante alertas y vulneraciones.

Los artículos 33, fracción VII de la Ley General de Protección, y 47, fracción VII de la Ley Estatal de Protección, disponen que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

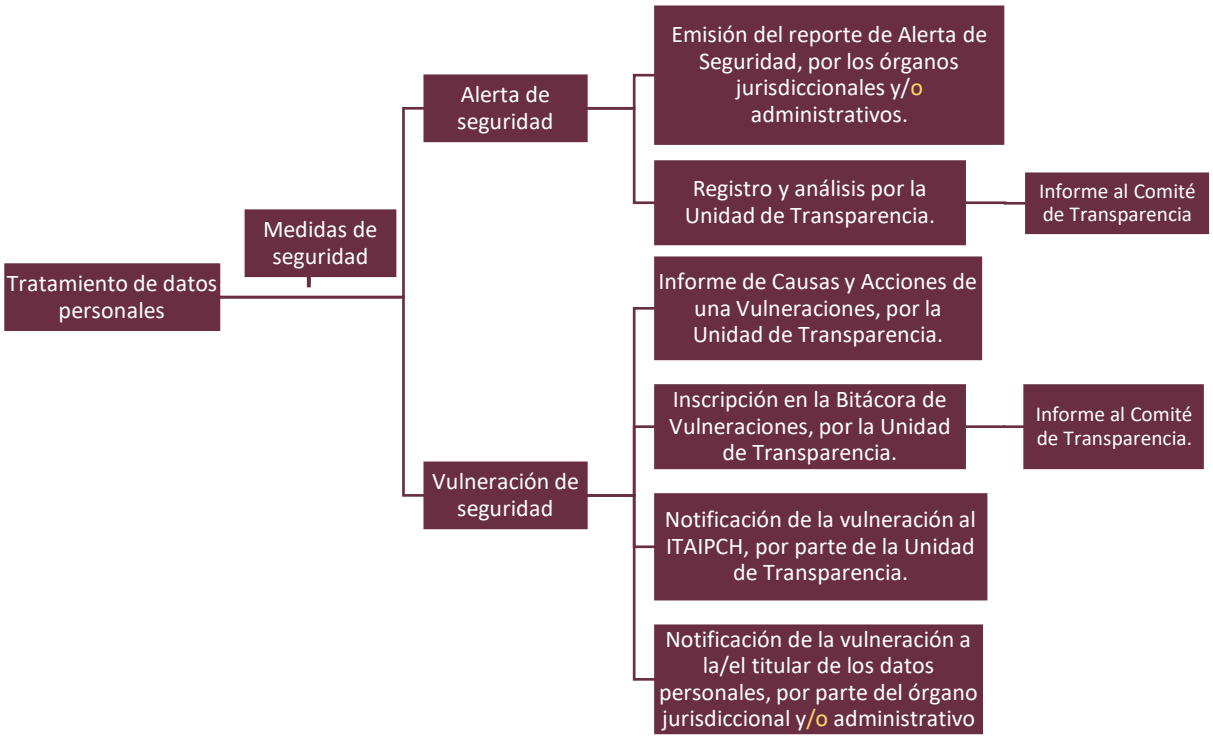
En ese sentido, el artículo 63, fracción VII de los Lineamientos Generales de Protección, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, la o el Oficial de Protección de Datos Personales deberá monitorear y revisar de manera periódica dichas medidas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar del Área de Informática.

Bajo ese panorama, en este documento se definen los mecanismos que los órganos jurisdiccionales y/o administrativos del TAPJECH, a través de la o el Oficial de Protección de Datos Personales, deberán operar ante el surgimiento de una alerta o vulneración en las medidas de seguridad de los datos personales.

Para la comprensión de los mecanismos referidos, se precisa la diferencia entre ambos conceptos como se muestra a continuación:

Alerta de seguridad	Vulneración de seguridad
Detección de una amenaza que, de haberse materializado en un daño, hubiera implicado una afectación en la seguridad de los datos personales.	Afectación acaecida a los datos personales en cualquier fase del tratamiento, que haya generado: 1. Su pérdida o destrucción no autorizada. 2.- El robo, extravío o copia no autorizada. 3.- El uso, acceso o tratamiento no autorizado. 4.- El daño, la alteración o modificación no autorizada.
No implica la materialización de una vulneración.	Implica un daño a los activos del TAPJECH, como lo son las bases de datos, el personal, el hardware, software, archivos o documentos electrónicos o en papel.
Advierten una anomalía o cambio inesperado o no deseado.	Riesgo materializado que afecta de manera significativa los derechos patrimoniales o morales de las titulares de los datos personales.



Los mecanismos, se desarrollarán conforme al esquema anterior.

Expuesto lo anterior, se procede a presentar el mecanismo que los órganos jurisdiccionales y/o administrativos del TAPJECH deberán efectuar cuando:

I. Se materialice una alerta de seguridad en cualquier fase del tratamiento de datos personales; y/o,

II. Se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales.

Lo anterior, se desarrollará en la forma que se describe a continuación.

I. Alertas de seguridad de los datos personales.

El mecanismo que aquí se describe, resulta obligatorio para los órganos jurisdiccionales y/o administrativos que en ejercicio de sus funciones realicen el tratamiento de datos personales.

Los artículos 31, de la Ley General de Protección y 45 de la Ley Estatal de Protección, indican que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, se deberán 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, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El párrafo segundo del artículo 55 de los Lineamientos Generales de Protección, dispone que dichas medidas constituyen mínimos exigibles, por lo que podrán adoptarse las medidas adicionales que se estimen necesarias para brindar mayores garantías en la protección de los datos personales.

En ese sentido, y con el fin de maximizar la protección de los datos personales en posesión del TAPJECH, el presente mecanismo persigue los objetivos siguientes:

- Registrar las amenazas que configuren alertas de seguridad.

- Analizar las alertas de seguridad registradas, con la finalidad de definir estrategias para la prevención de una vulneración de seguridad.

- Integrar las estrategias de prevención en el Documento de Seguridad, a efecto de que se implementen como medidas adicionales de seguridad, según sea el caso.

Es importante destacar, que resultará indispensable identificar que efectivamente los hechos ocurridos constituyan una alerta a la seguridad de los datos personales, para lo cual, los órganos jurisdiccionales y/o administrativos deberán verificar la materialización de los supuestos siguientes:

- Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.

- Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para cada órgano jurisdiccional y/o administrativo.

Para ello, los órganos jurisdiccionales y/o administrativos, se auxiliarán del Área de Informática, requiriendo el soporte técnico y administrativo para la emisión de opiniones y/o dictámenes respectivos.

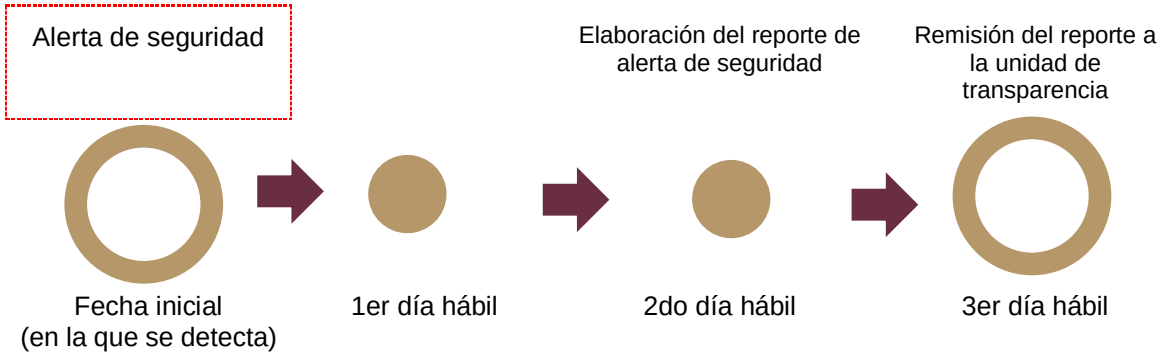
En mérito de lo anterior, en caso de advertir una alerta de seguridad se deberá proceder conforme al mecanismo siguiente:

A. Al segundo día hábil siguiente a la fecha en que se detecte la amenaza, el órgano jurisdiccional y/o administrativo respectivo deberá elaborar un Reporte de Alerta de Seguridad, en los términos que más adelante se abordarán.

B. Al tercer día hábil siguiente a la fecha en que se detecte la anomalía, el reporte deberá ser remitido a la o el Oficial de Protección de Datos Personales quien efectuará el análisis correspondiente.

Si del análisis de la alerta de seguridad, la o el Oficial de Protección de Datos Personales advierte la posibilidad de generar una estrategia de prevención, procederá a su integración en el Documento de Seguridad en el apartado respectivo.

Lo que precede, se representa de la forma siguiente:



Reporte de Alerta de Seguridad.

Una vez que el órgano jurisdiccional y/o administrativo advirtió un posible incidente en el tratamiento de los datos personales, deberá definir si este constituye una alerta de seguridad.

Se reitera que, para considerar la configuración de una alerta de seguridad, se deberán actualizar los supuestos siguientes:

- ✓ Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.

- ✓ Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para el órgano jurisdiccional y/o administrativo.

Para establecer lo anterior, se requerirá el soporte técnico y administrativo del Área de Informática, o en su caso al Área de Recursos Materiales y Servicios Generales con base en los artículos 62, fracciones I, XI y XXIV, y 64, fracción II y V del Reglamento Interior del TAPJECH.

Verificada la existencia de una alerta de seguridad, el órgano jurisdiccional y/o administrativo deberá emitir un Reporte de Alerta de Seguridad, en el cual se deberá considerar, como mínimo, el desarrollo de los aspectos siguientes:

1. **Detección**
   - ✓ Nombre, cargo y adscripción de la persona servidora pública que detectó la amenaza.
   - ✓ Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta.
   - ✓ Tratamiento o sistema en que ocurrió.
   - ✓ Nombre, cargo y adscripción de la persona servidora pública responsable del tratamiento o sistema.
   - ✓ Datos personales involucrados en la amenaza.
2. **Proyección de una posible vulneración**
   - ✓ Elementos que permitieron el desarrollo o persistencia de la amenaza.
   - ✓ Elementos que contuvieron el desarrollo o persistencia de la amenaza.
   - ✓ Actuaciones que pueden evitar la reincidencia de la amenaza.
   - ✓ Descripción de los efectos que hubiera causado la anomalía si hubiere persistido hasta materializar una vulneración.
3. **Medidas de seguridad involucradas**
   - ✓ Descripción clara de los controles físicos o electrónicos involucrados en la amenaza.
   - ✓ Circunstancias que, individual o conjuntamente, permitieron la existencia de la amenaza.

- ✓ Justificar si la amenaza pudo ser prevenida, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.

- ✓ Ante la materialización de la amenaza, justificar si en el futuro puede evitarse su reincidencia, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente puedan impedirlo.

- ✓ Si la forma de prevenir o evitar la reincidencia de la amenaza, involucran una nueva medida de seguridad, deberá ser claramente descrita.

Concluido lo anterior, al tercer día hábil siguiente a la detección de la alerta, el reporte deberá ser remitido a la o el Oficial de Protección de Datos Personales.

El formato del reporte de alerta de seguridad constituye el anexo 5 de este documento, al cual se le integrarán los informes que, en su caso, genere el Área de Informática y/o el Área de Recursos Materiales y Servicios Generales con base al soporte que brinde.

Registro y análisis de la alerta de seguridad.

Recibido el Reporte de Alerta de Seguridad, la o el Oficial de Protección de Datos Personales procederá a su registro y realizará un análisis que deberá dilucidar los aspectos siguientes:

- El impacto que tiene la alerta en la seguridad de los datos personales.

- Observaciones en materia de seguridad que el órgano jurisdiccional y/o administrativo debe observar en el futuro desarrollo del tratamiento.

- Medidas de seguridad adicionales que se estime conducente implementar.

Si resulta posible determinar una estrategia de prevención con los órganos jurisdiccionales y/o administrativos en las que la alerta de seguridad pueda desencadenarse.

Si del análisis de la alerta de seguridad, la o el Oficial de Protección de Datos Personales advierte la posibilidad de generar una estrategia de prevención, propondrá a la Unidad de Transparencia la integración en el Documento de Seguridad en el apartado respectivo, acorde a la autorización del Comité de Transparencia del TAPJECH.

II. Vulneraciones de seguridad de los datos personales.

El mecanismo que aquí se describe, resulta obligatorio para los órganos jurisdiccionales y/o administrativos que en ejercicio de sus funciones realicen el tratamiento de datos personales.

En primer término, de conformidad con lo establecido en el artículo 38 de la Ley General de Protección, en relación con el numeral 52 de la Ley Estatal de Protección, resulta indispensable que el órgano jurisdiccional y/o administrativo identifique que efectivamente los hechos ocurridos constituyan una vulneración a la seguridad de los datos personales, para lo cual, deberán verificar la materialización de los supuestos siguientes:

- Que exista una afectación concreta en el tratamiento de los datos personales que haya generado conjunta o separadamente los supuestos siguientes:

    1. La pérdida o destrucción no autorizada.
    2. El robo, extravío o copia no autorizada.
    3. El uso, acceso o tratamiento no autorizado.
    4. El daño, la alteración o modificación no autorizada.
    5. Otra vulnerabilidad considerada en el apartado referido en el presente Documento de Seguridad.

- Que la afectación implique un daño a las bases de datos, al personal, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para los órganos jurisdiccionales y/o administrativos del TAPJECH.

Para ello, los órganos jurisdiccionales y/o administrativos, se auxiliarán del Área de Informática y/o Área de Recursos Materiales y Servicios Generales, requiriéndole soporte técnico y administrativo para la emisión de opiniones y/o dictámenes respectivos, de los que pueda soportarse la materialización o no de los supuestos anteriores.

Si alguno de los puntos anteriores no se actualiza, no se considerará una vulneración de los tratamientos o sistemas de datos personales, razón por la cual no será necesario la ejecución del proceso descrito en este apartado, y deberá procederse, en su caso, en los términos previstos para una alerta de seguridad.

Ante una vulneración en la seguridad de los datos personales, los artículos 37, 38, 39, 40 y 41 de la Ley General de Protección, en relación con los dispositivos 52, 53, 54, 55 y 56 de la Ley Estatal de Protección, establecen las obligaciones siguientes:

- Analizar las causas por las cuales se presentó esa vulneración e implementar las respectivas Medidas de Seguridad, así como los buenos hábitos referidas en éstas, sobre las acciones preventivas y correctivas para adecuar dichas medidas y el tratamiento de los datos personales a efecto de evitar que la vulneración se repita.

- Inscribir la vulneración en la bitácora de control.

- Informar sin dilación alguna a la/el titular y al Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Chiapas, las vulneraciones que afecten de forma significativa derechos patrimoniales o morales. A fin de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos.

Se procede a describir la forma y tiempo en que se acreditará el cumplimiento de cada uno de los puntos que anteceden. Lo anterior, de conformidad con el esquema siguiente:

Análisis de las causas de la vulneración	Elaboración del Informe de Causas y Acciones en una Vulneración por el órgano jurisdiccional y/o administrativo: día hábil siguiente a partir de la detección de la vulneración.
	Remisión a la Unidad de Transparencia: segundo día hábil siguiente a partir de la detección de la vulneración.
Inscripción en la Bitácora de Vulneraciones	La unidad de Transparencia tendrá 24 horas a partir de que se le haya notificado la vulneración por parte del órgano jurisdiccional y/o administrativo respectivo.
Notificación al Órgano Garante local	La Unidad de Transparencia tendrá 72 horas a partir de que se detecte de la vulneración.
Notificación al/la titular afectada	El órgano jurisdiccional y/o administrativo, tendrá 72 horas a partir de que se detecte la vulneración.

Lo cual, se detalla en los apartados siguientes.

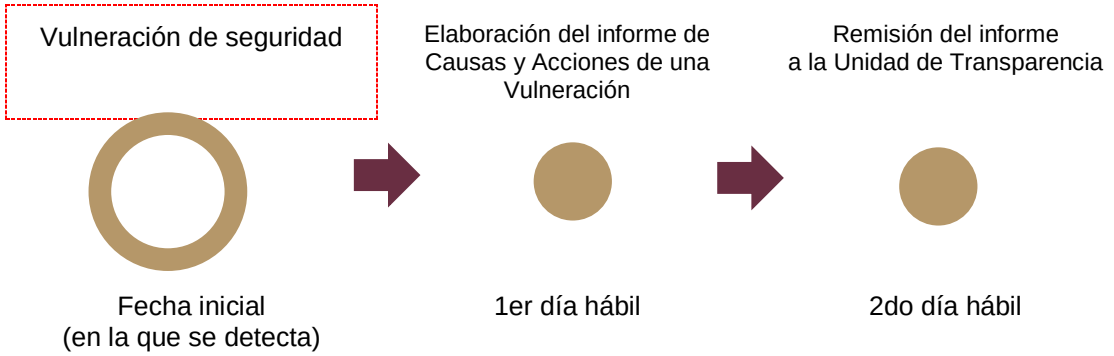
Análisis de las causas por las cuales se presentó la vulneración y de las acciones preventivas y correctivas correspondientes.

Una vez verificada la existencia de la vulneración, procederá a realizar lo siguiente:

I. Dentro del día hábil siguiente a la fecha en que se detecte, el órgano jurisdiccional y/o administrativo deberá elaborar un Informe de Causas y Acciones de una Vulneración, en los términos que más adelante se abordarán. En la que el órgano referente, debe soportarse con el dictamen u opinión técnica del Área de Informática y/o Área de Recursos Materiales y Servicios Generales.
II. Al segundo día hábil siguiente a la fecha en que se detecte, el órgano jurisdiccional y/o administrativo deberá remitir el informe a la Unidad

de Transparencia, quien efectuará el registro y análisis correspondiente.

Lo que precede, se representa de la forma siguiente:



Informe de Causas y Acciones de una Vulneración

Para la emisión del informe en mención, necesariamente habrá que considerar, como mínimo, el desarrollo de los aspectos siguientes:

1. Información general de la vulneración.

A. Detección

- ✓ Nombre, cargo y adscripción de la persona servidora pública que detectó la vulneración.
- ✓ Fecha, hora y lugar en que se detectó la vulneración.
- ✓ Tratamiento o sistema que fue vulnerado.
- ✓ Nombre, cargo y adscripción de las personas servidoras públicas responsables del tratamiento o sistema.
- ✓ Datos personales involucrados en la vulneración.
- ✓ Descripción detallada de la forma en que se detectó la vulneración.

B. Investigación

- ✓ Fecha y hora en que se inició la investigación de la vulneración.

- ✓ Nombre y cargo de la persona servidora pública designada para la investigación de la vulneración.
- ✓ Naturaleza de la vulneración.
- ✓ Fecha y hora de la vulneración.
- ✓ Descripción detallada de la forma en que se desarrolló la vulneración.
- ✓ Descripción detallada de las afectaciones que fueron materializadas.
- ✓ Tipo y número aproximado de personas titulares afectadas.
- ✓ Posibles consecuencias de la vulneración.

C. Medidas de seguridad vulneradas e impacto causado

- ✓ Descripción clara de cada uno de los controles físicos o electrónicos que operan en el tratamiento o sistema, incluyendo la persona servidora pública responsable de su implementación.
- ✓ Identificación de la totalidad de las personas que cuentan con acceso a cualquiera de las fases del tratamiento, incluyendo personas servidoras públicas o personas ajenas al TAPJECH.
- ✓ Identificación y descripción de la vulneración materializada.
- ✓ Determinación del nivel de impacto causado por la vulneración en relación con el tratamiento o sistema (alto, medio, bajo), considerando el número de titulares afectadas, así como el tipo y naturaleza de los datos personales involucrados en la vulneración.
- ✓ Determinación relativa a si la vulneración generó una afectación significativa a los derechos patrimoniales y/o morales de las titulares de los datos personales.

De conformidad con lo previsto en los párrafos tercero y cuarto del artículo 66 de los Lineamientos Generales de Protección, para determinar la existencia de una afectación significativa patrimonial o moral, se deberán atender los siguientes criterios:

Afectación Patrimonial	Afectación Moral
La vulneración se encuentra relacionada, de manera enunciativa más no limitativa, con: ▪ Los bienes muebles e inmuebles. ▪ Información fiscal. ▪ Historial crediticio. ▪ Ingresos y egresos. ▪ Cuentas bancarias. ▪ Seguros. ▪ Afores. ▪ Fianzas. ▪ Servicios contratados. ▪ Cantidades o porcentajes relacionados con la situación económica del/la titular.	La vulneración esté relacionada, de manera enunciativa más no limitativa, con: ▪ Sentimientos. ▪ Afectos. ▪ Creencias. ▪ Decoro. ▪ Honor. ▪ Reputación. ▪ Vida privada. ▪ Configuración y aspectos físicos. ▪ Consideración que de sí mismo tienen los demás. ▪ La que menoscabe ilegítimamente la libertad o la integridad física o psíquica del/la titular.

2. Acciones preventivas y correctivas.

- Justificar si la vulneración pudo ser prevenida, es decir, si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente efectivamente hubiera podido llevar a cabo tal prevención.

- Si la vulneración no pudo ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con lo que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.

- Analizar las medidas que, de acuerdo a la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.

- Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración.

- Recomendaciones para la persona titular afectada.

- Medio informativo a través del cual se consulte mayores datos respecto a la vulneración.

- Datos de contacto de las personas servidoras públicas designadas para la gestión de la vulneración.

- Cualquier información y/o documentación que se considere conveniente.

Hecho lo anterior, al segundo día hábil siguiente a la fecha en que se detectó la vulneración, el órgano jurisdiccional y/o administrativo deberá remitir el informe a la o el Oficial de Protección de Datos Personales, quien efectuará el registro y análisis correspondiente.

Durante el proceso de detección, investigación, medidas de seguridad vulneradas e impacto causado respecto a las vulneraciones, así como de las acciones preventivas y correctivas, el órgano referente, y la Unidad de Transparencia, se soportarán con el dictamen u opinión técnica del Área de Informática y/o Área de Recursos Materiales y Servicios Generales.

El formato del referido informe constituye el anexo 6 de este documento.

Análisis de la vulneración de seguridad.

Recibido el Informe de Causas y Acciones de una Vulneración, la o el Oficial de Protección de Datos Personales procederá a su registro y realizará un análisis que deberá dilucidar los aspectos siguientes:

- El impacto que tiene la vulneración de seguridad en la protección de los datos personales.

- Observaciones en materia de seguridad que el órgano jurisdiccional y/o administrativo debe observar en el futuro desarrollo del tratamiento.

- Medidas de seguridad adicionales que se estimen conducentes implementar.

- Si resulta posible determinar una estrategia de prevención en diversos tratamientos en los que la vulneración de seguridad pueda desencadenarse.

Si del análisis de la vulneración, la o el Oficial de Protección de Datos Personales advierte la posibilidad de generar una estrategia de prevención, hará la propuesta respectiva a la Unidad de Transparencia, y esta procederá a su integración en el Documento de Seguridad en el apartado respectivo, previa autorización que el Comité de Transparencia determine.

Inscripción en la bitácora de vulneraciones.

De conformidad con el artículo 39 de la Ley General de Protección, en relación con el numeral 53 de la Ley Estatal de Protección, se deberá llevar una bitácora de las vulneraciones a la seguridad en la que se realice una descripción de ésta, la fecha en que ocurrió, su motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

En ese sentido, la o el Oficial de Protección de Datos Personales propondrá a la Unidad de Transparencia la integración de la Bitácora de Vulneraciones a la Seguridad de los Datos Personales, en la que se concentrarán las vulneraciones acaecidas en la totalidad de los órganos jurisdiccionales y/o administrativos del TAPJECH; lo anterior, de conformidad con el formato que constituye el anexo 7 de este documento.

Por lo que, dentro del plazo de 24 horas siguientes al en que el órgano jurisdiccional y/o administrativo notifique la vulneración, se deberá proceder a su registro.

La inscripción realizada, deberá ser informada por la Unidad de Transparencia al Comité de Transparencia, para su conocimiento y efectos conducentes.

Posterior a la inscripción deberá remitirse una copia de dicho registro al órgano jurisdiccional y/o administrativo, a efecto de que sea integrada a su bitácora interna de incidentes y vulneraciones a la seguridad.

Informe de la vulneración al Órgano Garante local, y al titular de los datos personales.

El artículo 40 de la Ley General de Protección, en relación con el numeral 54 de la Ley Estatal de Protección dispone que, ante una vulneración que afecte de forma significativa derechos patrimoniales o morales, se deberá informar sin dilación alguna al/la titular y al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

Dicho informe, deberá realizarse en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que las/los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Al respecto, el artículo 66 de los Lineamientos Generales de Protección estipula que la notificación del informe al/la titular y al Instituto referido deberá realizarse dentro en un plazo máximo de 72 horas, a partir de que se confirme la ocurrencia de la vulneración y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

Bajo ese panorama, ocurrida una vulneración, la Unidad de Transparencia deberá realizar lo siguiente:

A. Notificar la vulneración al Órgano Garante Local.

B. Verificar que el órgano jurisdiccional y/o administrativo respectivo notifique al titular o titulares afectados por la vulneración identificada.

Lo anterior, en los términos que se explican a continuación.

Notificación de la vulneración al Órgano Garante Local.

La Unidad de Transparencia analizará de forma exhaustiva las particularidades de la vulneración y, de conformidad con el artículo 66 de los Lineamientos Generales de Protección, realizará lo siguiente:

- Identificará si en el Informe de Causas y Acciones de una Vulneración, el órgano jurisdiccional y/o administrativo respectivo consideró que la afectación sufrida causaba un daño significativo patrimonial o moral en detrimento de las titulares de los datos personales afectadas.

- Supervisará las acciones implementadas por el órgano jurisdiccional y/o administrativo respectivo para restituir la seguridad del tratamiento de los datos personales.

Por ello, en términos de lo establecido en los artículos 40 y 41 de la Ley General de Protección, en relación con los artículos 54 y 55 de la Ley Estatal de Protección, en caso de que el órgano jurisdiccional y/o administrativo haya considerado que la afectación al patrimonio o la moral causada es significativa, dentro de las 72 horas siguientes a la confirmación de la ocurrencia de la vulneración, la Unidad de Transparencia realizará un informe dirigido al Órgano Garante Local que considere los aspectos siguientes:

- La hora y fecha de la identificación de la vulneración.
- La hora y fecha del inicio de la investigación sobre la vulneración.
- La naturaleza de la vulneración ocurrida.
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
- Las categorías y número aproximado de personas titulares afectadas.
- Los sistemas de tratamiento y datos personales comprometidos.
- Las acciones correctivas realizadas de forma inmediata.
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
- Las recomendaciones dirigidas a la/el titular.
- El medio puesto a disposición de la/el titular para que pueda obtener más información al respecto.

- El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Órgano Garante Local.
- Cualquier otra información y documentación que se considere conveniente hacer del conocimiento del Órgano Garante Local.

Notificación de la vulneración a la/el titular de los datos personales.

De haberse considerado la actualización de una afectación significativa al patrimonio o a la moral de la/el titular o titulares de los datos personales, el órgano jurisdiccional y/o administrativo respectivo deberá realizar un informe que considere los aspectos siguientes:

- La naturaleza de la vulneración.
- Los datos personales comprometidos.
- Las recomendaciones a la/el titular acerca de las medidas que este pueda adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener más información al respecto.
- La descripción de las circunstancias generales en torno a la vulneración ocurrida, que le ayuden a entender el impacto de la vulneración.
- Cualquier otra información y documentación que se considere conveniente para apoyar a las titulares de los datos personales afectadas.

La Unidad de Transparencia podrá auxiliar al órgano jurisdiccional o administrativo en la elaboración del informe, el cual deberá notificar a la/el titular o los titulares afectados dentro de las 72 horas siguientes a la detección de la vulneración.

Dicha notificación, deberá efectuarse a través del medio que resulte idóneo y de fácil acceso, considerando la forma en que se obtuvieron los datos personales, el perfil que guarda la/el titular y la forma en que se mantiene contacto con él y en ninguno de los casos, deberá generarle costo alguno;

lo anterior, en los términos establecidos en el artículo 68 de los Lineamientos Generales de Protección.

Hecho lo anterior, la instancia respectiva deberá remitir al órgano jurisdiccional y/o administrativo el acuse de recibo o cédula de notificación correspondiente.

C. Mecanismo de auditoría en la materia.

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V de la Ley General de Protección, en relación con el numeral 44, fracción V de la Ley Estatal de Protección, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permitan comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales de Protección, dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.

Por tanto, con la finalidad de comprobar el cumplimiento de las políticas de protección de datos personales, así como para monitorear y revisar la eficacia y eficiencia del sistema de gestión, se elaboró el presente Mecanismo de Auditoría en Materia de Datos Personales.

I. Finalidades y objetivos

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

- Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable.
- Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión y el Documento de Seguridad.

- Verificar la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas.

- Validar el avance de los objetivos planteados en el presente Documento de Seguridad.

- Prevenir la materialización de vulneraciones a la seguridad de los datos personales.

- Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.

En ese sentido, el Mecanismo de Auditoría en Materia de Datos Personales tiene como objetivos principales los siguientes:

1. Determinar la forma en que se desarrollarán las etapas de las auditorías en materia de datos personales.
2. Establecer los aspectos a examinar.
3. Puntualizar los documentos a través de los cuales se asentará el desarrollo de las etapas respectivas, las observaciones advertidas y las aclaraciones conducentes.
4. Precisar el proceso a través del cual se seleccionarán los órganos jurisdiccionales y/o administrativos auditables.

Es importante referir que el alcance que tendrán las auditorías practicadas se concentrará exclusivamente en el análisis de la forma en que cada órgano jurisdiccional y/o administrativo, en el ámbito de su competencia, implementa las políticas que les resulten aplicables en materia de datos personales, así como la evaluación del estado de seguridad en que se encuentran los datos personales bajo su tratamiento; lo anterior, con la finalidad de implementar mejoras que de manera progresiva permitan al TAPJECH perfeccionar el manejo y protección de los datos personales.

II. Instancia ejecutora del programa y ámbito de aplicación.

Respecto de la ejecución del Programa, debe referirse que para adoptar los mecanismos previstos en el artículo 30, fracción V, de la Ley General de Protección, en relación con el numeral 44, fracción V de la Ley Estatal de

Protección, la Unidad de Transparencia, debe establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.

Consecuentemente, el Programa de Auditoría en materia de Datos Personales será ejecutado por la Unidad de Transparencia.

Por lo que se refiere al ámbito de aplicación, se indica que los órganos jurisdiccionales y/o administrativos del TAPJECH que en ejercicio de sus funciones realicen el tratamiento de datos personales, serán los sujetos auditables, de modo que se encuentran obligadas a coadyuvar activamente con la Unidad de Transparencia para el desarrollo de las auditorías respectivas.

III. Etapas de las auditorías en materia de datos personales

Las auditorías en materia de protección de datos personales estarán conformadas por las etapas de apertura, revisión y conclusiones. Dentro del desarrollo de éstas, la Unidad de Transparencia se auxiliará del personal del Área de Informática, Área de Recursos Materiales y Servicios Generales, Área Coordinadora de Archivos, así como de la Contraloría del TAPJECH, a efecto de contar debidamente con las facultades pertinentes.

La etapa de apertura tendrá la finalidad de definir el personal del órgano jurisdiccional y/o administrativo auditado ante el cual la Unidad de Transparencia substanciará la auditoría, así como los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial o virtual), y los requerimientos específicos necesarios para su realización.

En la etapa de revisión se realizará el escrutinio de la forma en que el órgano jurisdiccional y/o administrativo acredita el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad, de conformidad con lo previsto en la normativa aplicable, así como en el Documento de Seguridad.

En la etapa conclusiva, la Unidad de Transparencia puntualizará al órgano jurisdiccional y/o administrativo auditado las consideraciones efectuadas,

abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y señalará la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que los órganos jurisdiccionales y/o administrativos deberán remitir las evidencias correspondientes.

a) Etapa de apertura

Notificación de auditoría

De conformidad con el calendario de auditorías en materia de datos personales, la Unidad de Transparencia, comunicará por oficio al órgano jurisdiccional y/o administrativo correspondiente, lo siguiente:

I. La fecha en que dará inicio la auditoría, la cual deberá realizarse con un mínimo de 5 días hábiles entre la notificación del oficio y su celebración.
II. La necesidad de que el órgano jurisdiccional y/o administrativo auditado designe al personal con el que la Unidad de Transparencia substanciará la auditoría.
III. La convocatoria a una reunión previa al inicio de la auditoría, entre el personal de la Unidad de Transparencia y el personal designado por el órgano jurisdiccional y/o administrativo a auditar.

Reunión previa

En el día señalado para la reunión previa, se informarán los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial, virtual o mixta), así como los requerimientos específicos necesarios para la realización de la propia auditoría.

Efectuada la reunión previa, la Unidad de Transparencia, elaborará una minuta en la que se precisará el desarrollo de la misma, la cual deberá ser signada por los involucrados.

Acuerdo de inicio

En el día estipulado para el comienzo de la auditoría, la Unidad de Transparencia, en conjunto con la o el Oficial de Protección de Datos

Personales emitirá un acuerdo de inicio en el que deberá asentar lo siguiente:

I. El día en que comenzará y finalizará la auditoría.

II. La persona servidora pública designada por la Unidad de Transparencia para sustanciar la auditoría.

III. La persona servidora pública designada por el órgano jurisdiccional y/o administrativo auditado para sustanciar la auditoría.

IV. La identificación del tratamiento o tratamientos de datos personales materia de la auditoría.

V. El tipo de revisión que amerite el tratamiento (documental, presencial, virtual o mixta).

VI. La documentación, sistema o espacio físico que deberá estar plenamente disponible para ser examinado.

VII. Los datos de contacto de la Unidad de Transparencia y de la o el Oficial de Protección de Datos Personales, ante los cuales podrán solventarse dudas relacionadas con el desarrollo de la auditoría.

El acuerdo de inicio deberá ser notificado al órgano jurisdiccional y/o administrativo respectivo y deberá obrar en el expediente que para esos efectos integre la Unidad de Transparencia.

b) Etapa de revisión

Esta etapa corresponde el escrutinio de la forma en que los órganos jurisdiccionales y/o administrativos acreditan el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad.

Examinación

En el marco de lo dictado en el acuerdo de inicio, la Unidad de Transparencia procederá a la revisión del tratamiento o tratamientos de datos personales, a efecto de corroborar que se encuentren apegados a los principios y deberes siguientes:

A. Principio de licitud: el tratamiento de datos personales deberá tener sustento o estar relacionado con las facultades o atribuciones que la normatividad aplicable confiera al órgano jurisdiccional y/o administrativo auditado.

B. Principio de finalidad: el tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera al órgano jurisdiccional y/o administrativo auditado.

C. Principio de lealtad: que los datos personales no se hayan obtenido, a través de medios engañosos o fraudulentos.

D. Principio de consentimiento: cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la Ley General de Protección, en relación con el numeral 18 de la Ley Estatal de Protección, el órgano jurisdiccional y/o administrativo, auditado deberá contar con el consentimiento previo de la/el titular para el tratamiento de los datos personales.

E. Principio de calidad: que el órgano jurisdiccional y/o administrativo auditado haya adoptado las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

F. Principio de proporcionalidad: que el órgano jurisdiccional y/o administrativo auditado sólo haya tratado los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad para la cual fueron recabados.

G. Principio de información: que el órgano jurisdiccional y/o administrativo auditado haya informado a la/el titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

H. Principio de responsabilidad: que el órgano jurisdiccional y/o administrativo auditado haya adoptado la políticas y mecanismos necesarios para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General de Protección, la

Ley Estatal de Protección, el Sistema de Gestión de Seguridad, así como del Documento de Seguridad del TAPJECH.

I. Deber de seguridad: que el órgano jurisdiccional y/o administrativo auditado haya establecido y mantenido medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión.

J. Deber de confidencialidad: el órgano jurisdiccional y/o administrativo auditado deberá demostrar la existencia de controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos.

Documento de conclusiones

La Unidad de Transparencia elaborará el documento de conclusiones, en el cual asentará la información que derive de la examinación realizada.

Dicho documento, deberá exponer de manera clara lo siguiente:

- La estimación de cumplimiento correspondiente a cada principio y deber.
- Consideraciones que se estimen relevantes en cuanto al tratamiento de los datos personales.
- Recomendaciones en materia de seguridad de los datos personales.
- Observaciones y requerimientos que deban ser atendidos ante una deficiencia, desviación o mejora necesaria en el tratamiento de los datos personales, especificando el plazo en que los órganos jurisdiccionales y/o administrativos deberán remitir las evidencias respectivas a la Unidad de Transparencia.
- Conclusiones generales de la auditoría.

c) Etapa conclusiva

Reunión final

La Unidad de Transparencia convocará al órgano jurisdiccional y/o administrativo auditado a una reunión final, con el objetivo de hacerle entrega del documento de conclusiones.

En tal reunión se explicarán a detalle las consideraciones efectuadas, se abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y se puntualizará el plazo y la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que los órganos jurisdiccionales y/o administrativos deberán remitir las evidencias correspondientes.

Efectuada la reunión final, la Unidad de Transparencia elaborará una minuta en la que se concentrarán las conclusiones alcanzadas, la cual deberá ser signada por las personas servidoras públicas involucradas.

Cumplimiento de observaciones y requerimientos

Dentro del plazo otorgado en el documento de conclusiones, el órgano jurisdiccional y/o administrativo auditado deberá remitir a la Unidad de Transparencia las evidencias del cumplimiento de las observaciones y requerimientos que le hubieran sido realizados.

Tales evidencias serán examinadas a efecto de dilucidar si cumplen con los extremos determinados y con ello, se atendió la deficiencia, desviación o mejora en el tratamiento de los datos personales.

Si de su examen la Unidad de Transparencia corrobora que han sido adecuadamente cumplidas las observaciones y requerimientos, se procederá al cierre de la auditoría.

Por el contrario, de concluir que existen extremos no cumplidos total o parcialmente, la Unidad de Transparencia realizará un único requerimiento

adicional, reiterando la forma en que el órgano jurisdiccional y/o administrativo auditado debe demostrar su cumplimiento.

Si a pesar de ello persiste el incumplimiento, la Unidad de Transparencia hará constar la persistencia de la deficiencia o desviación y procederá al cierre de la auditoría.

Informe de cierre de la auditoría

Teniendo a la vista la documentación generada en las etapas de la auditoría, la minuta de la reunión final y las evidencias que deriven del cumplimiento de observaciones y requerimientos, la Unidad de Transparencia elaborará un informe final con el cual se dará por concluida la auditoría.

Cabe precisar que, si del informe efectuado se advierte un incumplimiento a las observaciones y requerimientos efectuados, se dará cuenta al Comité de Transparencia, a efecto de que tome conocimiento de tal inobservancia, así como de la deficiencia o desviación en el tratamiento respectivo.

Dicho informe, deberá ser notificado al órgano jurisdiccional y/o administrativo auditado a más tardar dentro de los tres días hábiles siguientes a su emisión.

Selección de los órganos jurisdiccionales y/o administrativos auditables

La programación de las auditorías se realizará a través de una selección de los órganos jurisdiccionales y/o administrativos, a propuesta del Comité de Transparencia al Pleno del TAPJECH, y conforme al panorama general de los tratamientos de los datos personales en el TAPJECH.

De manera que, las auditorías a practicar se programarán analizando dicho panorama a la luz de criterios de selección específicos.

Panorama general

Del Inventario de Datos Personales y Sistemas, se tomará en consideración lo siguiente:

- El número de órganos jurisdiccionales y/o administrativos involucrados en el tratamiento de datos personales.

- El número de tratamientos que cada órgano jurisdiccional y/o administrativo realiza, así como el resultado global de tal estadística.

- Los tratamientos se clasificarán en las categorías siguientes:
  - Datos de carácter identificativo.
  - Características personales.
  - Circunstancias sociales.
  - Datos académicos y profesionales.
  - Detalles del empleo, cargo o comisión.
  - Información comercial.
  - Datos económicos.
  - Financieros y de seguro.

- Órganos jurisdiccionales y/o administrativos que operen uno o varios tratamientos que conlleven datos personales sensibles.

Criterios de selección.

Ante el panorama general expuesto y atendiendo a los objetivos de este programa, los criterios de selección serán los siguientes:

I. Tratamientos con un número considerable de riesgos.

II. Tratamientos que, de ser objeto de una vulneración, tengan como consecuencia un impacto mayor a la/el titular de los datos personales.

III. Tratamientos prioritarios, especiales o estratégicos, que serán aquellos que conlleven un alto valor potencial cuantitativo y cualitativo para una tercera persona no autorizada para su posesión o que puedan causar un daño a la reputación del TAPJECH.

IV. Órganos jurisdiccionales y/o administrativos cuyas funciones impliquen un alto número de tratamientos.

V. Órganos jurisdiccionales y/o administrativos cuyas funciones impliquen el tratamiento de datos sensibles.

En su análisis se considerarán los factores siguientes:

- El riesgo inherente a cada dato personal de acuerdo a su categoría.
- La sensibilidad del dato personal.
- El desarrollo tecnológico del sistema que opera el tratamiento.
- Posible impacto y consecuencias de la vulneración del dato personal.
- Número de titulares.
- Vulneraciones previas ocurridas en el sistema de datos.
- Valor y exposición de los activos involucrados con el tratamiento.

Para fijar el impacto, se considerará el tipo de riesgo existente (operativo, normativo o tecnológico), su probabilidad (muy poco probable, poco probable, probable o segura) y la proyección del daño que pueden producirse si la amenaza se concreta.

Programación.

Realizada la selección de los órganos jurisdiccionales y/o administrativos bajo los criterios expuestos, el Comité de Transparencia ponderará la cronología que deberá seguir la calendarización de las auditorías.

Dicha calendarización se hará de conocimiento al Pleno del TAPJECH para su atención e instrucciones, que en su caso deriven, hacia la Unidad de Transparencia respecto a su implementación y seguimiento.

X.- Programa de capacitación en materia de Protección de Datos Personales

El artículo 33, fracción VIII, de la Ley General de Protección, en relación con el artículo 50, fracción XIX de la Ley Estatal de Protección, disponen 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 que se efectúe.

En ese sentido, a propuesta de la Unidad de Transparencia, en coordinación con las áreas administrativas competentes, el Comité deberá aprobar anualmente el programa de capacitación de datos personales.

Sin embargo, en aras de fomentar la cultura de protección de datos personales, la Unidad de Transparencia buscará el enlace de comunicación con el Órgano Garante Local, o a través de instituciones involucradas en la materia, y se lleven a cabo capacitaciones sobre los siguientes temas:

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
  - Dirigido a todas las personas servidoras públicas del TAPJECH.

- Sistema de Gestión de Seguridad de Datos Personales Sector Público.
  - Dirigido a las personas servidoras públicas responsables de los tratamientos que se llevan a cabo en el TAPJECH.

- Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales.
  - Dirigido a las personas servidoras públicas inmersas en dicho tratamiento, así como a las indicadas en el manejo de incidentes de seguridad en la materia, dentro del TAPJECH.

XI.- Actualización del Documento de Seguridad

Conforme al numeral 36 de la Ley General de Protección, en relación del dispositivo 51 de la Ley Estatal de Protección, se indica que los sujetos obligados deberán actualizar el documento de seguridad cuando ocurra alguno de los eventos siguientes:

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

En mérito de lo anterior, la Unidad de Transparencia procederá a la elaboración de un proyecto de actualización del documento de seguridad cuando se materialicen los supuestos siguientes:

- De la ejecución de cualquiera de los Mecanismos de Monitoreo, Revisión, Alertas y Auditoría, se desprenda la actualización de:
  - Una modificación sustancial a determinado tratamiento que derive en un cambio en su nivel de riesgo.
  - Una estrategia que maximice la seguridad de los datos personales que pueda ser aplicable a diversos órganos jurisdiccionales y/o unidades/áreas administrativas.
- Cuando se integre una política de seguridad de los datos personales en el Sistema de Gestión de Seguridad del TAPJECH.
- Cuando los órganos jurisdiccionales y/o unidades/áreas administrativas lo soliciten en virtud de la maximización o perfeccionamiento de una medida de seguridad determinada.

La Unidad de Transparencia rendirá un informe cada seis meses al Comité de Transparencia en el que detalle si hubo o no propuestas de actualización al Documento de Seguridad.

DISPOSICIONES TRANSITORIAS

Primera: El presente Documento de Seguridad del Tribunal Administrativo del Poder Judicial del Estado de Chiapas, entrará en vigor al día siguiente de su aprobación por el Pleno del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Segunda: Se deroga cualquier otra disposición que se oponga o contravenga a lo establecido en el presente instrumento.

Tercera: En los casos en que se presente controversia en cuanto a la interpretación, aplicación y observancia en el presente Documento de Seguridad, el Comité de Transparencia del Tribunal Administrativo del Poder Judicial del Estado de Chiapas resolverá lo conducente, conforme a los artículos 113 y 114 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Cuarta: Con relación al Plan de Trabajo del Documento de Seguridad, la Unidad de Transparencia recabará las opiniones necesarias para implementar las acciones relacionadas con este instrumento, considerando la materia de archivos, la estructura tecnológica y presupuestal, así como el programa de capacitación al interior del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Quinta: Publíquese el presente Documento de Seguridad en la página electrónica del Tribunal Administrativo del Poder Judicial del Estado de Chiapas.

Dado en el salón del Pleno del Tribunal Administrativo del Poder Judicial del Estado, en la Ciudad de Tuxtla Gutiérrez, Chiapas; a los 05 días del mes de septiembre del año 2023.

Magistrada Presidenta Susana Sarmiento López, Magistrada Mónica de Jesús Trejo Velázquez y Magistrado Víctor Marcelo Ruiz Reyna, ante la fe de la Secretaria General de Acuerdos y del Pleno Fabiola Antón Zorrilla.

SUSANA SARMIENTO LÓPEZ
MAGISTRADA PRESIDENTA

MÓNICA DE JESÚS TREJO VELÁZQUEZ
MAGISTRADA

VÍCTOR MARCELO RUIZ REYNA
MAGISTRADO

FABIOLA ANTÓN ZORRILLA
SECRETARIA GENERAL DE ACUERDOS Y DEL PLENO