



DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

**OFICINA DEL GOBERNADOR
JEFATURA DE OFICINA DE GUBERNATURA
COMITÉ DE TRANSPARENCIA**

OG/12C.10-UT/PDP-DS/2026



Las personas integrantes del Comité de Transparencia de la Oficina del Gobernador, en ejercicio de las facultades que confieren los artículos 40, fracciones I, IV y VIII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, 78, fracciones I, II, IV, V y VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas; y 1, 2, 6 y 11 del Reglamento Interior de la Oficina del Gobernador del Estado de Chiapas, 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, derecho del cual surgen 4 vertientes principales, como 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 relación con lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas establecen 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 la Oficina del Gobernador del Estado de Chiapas.

Asimismo, es de precisarse que la reforma a la Constitución Política de los Estados Unidos Mexicanos a través del Decreto por el que se reforman diversas disposiciones en materia de simplificación orgánica, publicado en el Diario Oficial de la Federación el día 20 de diciembre de 2024, estableció diversas acciones de actualización a nivel estatal en Chiapas, así como en lo local e internamente por cada sujeto obligado.

En esa tesitura, la Oficina del Gobernador (antes Gubernatura), determinó en su interior, las disposiciones relativas a las medidas de seguridad en materia de protección de datos personales. Sin embargo, derivado del cambio de administración (08 de diciembre de 2024) en el Poder Ejecutivo del Estado, trajo consigo la necesidad de generar agentes de cambio que permitan establecer medidas de seguridad relacionadas con las condiciones actuales y en apego a su normatividad vigente.

Por lo anterior, como bien lo señala la normatividad de la materia como una de las causales de actualización al presente instrumento, surge la necesidad de realizar las adecuaciones necesarias acordes a la normatividad y estructura orgánica, lo que trasciende transversalmente en favor de la ciudadanía y de las personas servidoras del pueblo.

El presente documento que tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior de la Oficina del Gobernador, por los órganos 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.

Atendiendo lo anterior, este organismo público 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 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 de la Oficina del Gobernador del Estado de Chiapas, pues tal y como lo dispone la Ley de la materia, 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, la Oficina del Gobernador comprometida con la tutela de los datos personales que trata, y en consonancia con lo establecido en la normatividad en la materia, así como las recomendaciones y cursos recibidos por la autoridad garante local, Transparencia para el Pueblo de Chiapas, órgano desconcentrado jerárquicamente subordinado de la Secretaría Anticorrupción y Buen Gobierno del Estado, que han impulsado 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, tendientes 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.

En virtud de lo anterior, en materia de protección de datos personales, las personas integrantes del Comité de Transparencia expiden el Documento de Seguridad, acorde a lo siguiente:

ÍNDICE

I.- Disposiciones generales.....	4
II.- Objeto y alcance del Documento de Seguridad.....	5
III.- Relevancia y base del Documento: Deber de Seguridad.....	6
IV.- Medidas de Seguridad de los Datos Personales de la Oficina	7
V.- Funciones y obligaciones del personal que trate datos personales	12
VI.- De las Vulnerabilidades	14
VII.- Inventario de Tratamientos y de Datos Personales de la Oficina	15
VIII.- Análisis de Riesgo y de Brecha.....	19
IX.- Plan de Trabajo.....	20
X.- Mecanismos de monitoreo y revisión	21
A. Mecanismo de monitoreo y supervisión.....	23
B. Mecanismos de actuación ante alertas y vulneraciones.	26
Sobre las auditorías en la materia.....	41
XI.- Programa de capacitación en materia de Protección de Datos Personales	41
XII.- Actualización del Documento de Seguridad	42
DISPOSICIONES TRANSITORIAS.....	43

I.- Disposiciones generales

Además de las disposiciones establecidas en el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, y de acuerdo con el Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales de la Oficina del Gobernador, en este ordenamiento se entenderá por:

Unidad de Informática: a la instancia dependiente de la Coordinación Administrativa de la Oficina del Gobernador, encargada de vigilar el cumplimiento de las normas, políticas y procedimientos que en materia de informática se establezca, conforme a lo señalado en el artículo 34 de su Reglamento Interior.

Área de Recursos Materiales y Servicios Generales: a la instancia dependiente de la Unidad de Apoyo Administrativo de la Coordinación Administrativa de la Oficina del Gobernador, encargada de implementar los mecanismos de control de los bienes patrimonio y en posesión de la Oficina, conforme a lo señalado en el artículo 32 de su Reglamento Interior.

Grupo Interdisciplinario: al grupo 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 de la Oficina del Gobernador.

Transparencia de Chiapas y/o Autoridad Garante Local: al órgano desconcentrado dependiente y jerárquicamente subordinado de la Secretaría Anticorrupción y Buen Gobierno del Estado de Chiapas, denominado Transparencia para el Pueblo de Chiapas, que funciona como autoridad garante local para los sujetos obligados que forman parte del Poder Ejecutivo del Estado de Chiapas, en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

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

Órganos administrativos: a las secretarías, coordinaciones, direcciones y demás órganos que auxilian en la labor de la Oficina del Gobernador.

Sistema de Gestión: al presente Sistema de Gestión de Seguridad de Protección de Datos Personales de la Oficina del Gobernador, 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 de este organismo público.

Titular: a la persona física o moral, o servidora pública titular de los datos personales.

Oficina: a la Oficina del Gobernador.

Unidad de Transparencia: a la Unidad de Transparencia de la Oficina del Gobernador, con las funciones delimitadas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y demás normatividad aplicable.

Área administrativa: a la Coordinación Administrativa de la Oficina del Gobernador, encargada de administrar y controlar el presupuesto de egresos autorizado para cada ejercicio, de acuerdo con la normatividad aplicable, así como para proponer medidas que tiendan a la preservación y al mejoramiento administrativo de la Oficina del Gobernador.

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 de la Oficina 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 administrativos, conforme a lo establecido en 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 Secretaría Privada, la Jefatura de Oficina de Gubernatura, la Coordinación Administrativa, la Coordinación de Asesores y Proyectos Estratégicos, la Coordinación de Giras, Logística, Ayudantía, Protocolo y Cultura Cívica, la Coordinación de Atención Ciudadana, la Representación del Gobierno del Estado de Chiapas en la Ciudad de México, así como los demás órganos administrativos 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 administrativos citados 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 administrativos que realicen tratamientos de datos personales.

En atención a ello, se hace saber a las personas servidoras públicas de la Oficina 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: oficinadelgovernador@transparencia.chiapas.gob.mx y/o direccion_informacion@atencionciudadana.chiapas.gob.mx

Vía telefónica: 9616188050, ext. 21218.

Vía presencial: en la Unidad de Transparencia ubicada en las oficinas que ocupan la Coordinación de Atención Ciudadana de la Oficina del Gobernador, planta baja del Edificio Sede de Gobierno, Colonia Centro, Ciudad de Tuxtla Gutiérrez, Chiapas, código postal 29000.

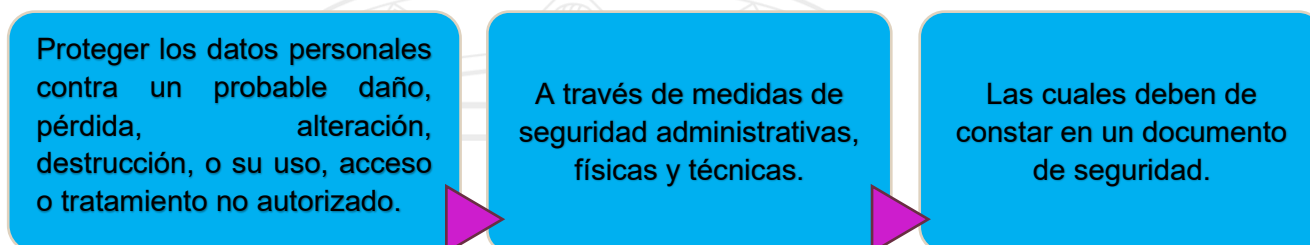
III.- Relevancia y base del Documento: Deber de Seguridad

El artículo 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, la Oficina 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 su uso, acceso o tratamiento no autorizado.
- Garantizar su confidencialidad, integridad y disponibilidad.

En ese sentido, los artículos 3, fracciones XIII, XVII, XVIII, XIX y XX, 26 y 29 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, la Oficina (a través de sus órganos administrativos responsables) debe realizar lo siguiente:



Lo anterior, conservando su confidencialidad, integridad y disponibilidad.

IV.- Medidas de Seguridad de los Datos Personales de la Oficina

Para el tratamiento de los datos personales que lleva a cabo la Oficina 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 Estatal de Protección, y lo contemplado en los Lineamientos Generales de Protección.

En tal virtud, la Oficina, partiendo de los resultados y oportunidades del primer Documento de Seguridad, inició 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 administrativa de este Organismo.

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, como norma general jurídica-administrativa que funge como eje rector en el actuar de las personas titulares de los órganos administrativos de la Oficina del Gobernador, lo es el Reglamento Interior de dicha Oficina, dado que, así como lo dispone su Decreto de creación, este Órgano es de apoyo directo del Ejecutivo, brindando asistencia inmediata en el desarrollo de sus actividades, así como vigilar y dar puntual seguimiento a las órdenes y acuerdos que expresamente le encomiende.

En su actuar, el personal, que formen parte del quehacer institucional de la Oficina del Gobernador, 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 Honestidad y Ética de los servidores públicos del Gobierno del Estado de Chiapas.

En ese contexto, la responsabilidad de cada tratamiento a los datos personales que se desarrollan en cada instancia de la Oficina, 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 de la Oficina, que intervienen en el tratamiento conocen a través de las disposiciones que 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 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 lo previsto en el artículo 47, fracción IV de la Ley Estatal de Protección, los órganos administrativos de la Oficina, 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 personas 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; 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, así como 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.

Las medidas de seguridad generales implementadas por la Oficina se clasifican en: administrativas, físicas, y técnicas, conforme a lo siguiente:

1. Administrativas:

- a. Estructura orgánica y organigrama general de los órganos de la Oficina.
- b. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.
- c. 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 de la Oficina.

2. Físicas:

- a. Resguardo de documentos e información en archivos físicos de trámite y concentración.
- b. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
- c. Limitar el número de personas con acceso a archivos físicos.
- d. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

- e. 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:

- a. Utilizar claves de usuario y contraseñas de manera personal, evitando compartirlas, prestarlas o registradas a la vista de otras personas.
- b. 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.
- c. Notificar de manera inmediata a la Unidad de Informática de la Coordinación Administrativa, 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.
- d. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
- e. 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.
- f. 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.
- g. 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.
- h. 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.

- i. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que no son necesarios para el desarrollo de funciones.
- j. 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.
- k. Las estipuladas por las personas servidoras públicas en ejercicio de las facultades y responsabilidades inherentes a su cargo, entre las que se destacan:
 - El acceso a los datos personales se condiciona al personal autorizado.
 - Contraseña particular para las personas servidoras públicas con acceso autorizado.
 - Contraseña única para el acceso a los datos personales.

Relativo a los buenos hábitos internos que debe realizar cada órgano 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.

V.- Funciones y obligaciones del personal que trate datos personales

Para garantizar que el tratamiento de los datos personales se realice de manera adecuada, correlacionada con las medidas y procedimientos contemplados en este instrumento, es necesario definir las responsabilidades de las personas involucradas en dicho tratamiento, teniéndolas debidamente identificadas y se haga constar.

En esa tesitura, conforme al artículo 57 de los Lineamientos Generales de Protección, el sujeto obligado responsable, a través de sus órganos administrativos, deberá establecer y documentar los roles específicos de las personas involucradas, conforme a la naturaleza del cumplimiento de los principios y deberes de la materia, definido en el Sistema de Gestión.

Por ende, esta Oficina establece las obligaciones y funciones nivelándolo en específico y en lo general, como se señala a continuación:

1. De forma específica, en el inventario de los sistemas de tratamiento de datos personales, se considera un apartado explicativo que indica a las personas servidoras públicas responsables del tratamiento por cada órgano administrativo.

Respecto a ello, las personas servidoras públicas identificadas señaladas por cada órgano administrativo, cada persona titular de estas últimas verificó que contaran con atribuciones y el perfil de puesto idóneo.

2. De manera general, las personas servidoras públicas involucradas en el tratamiento de datos personales en nombre de la Oficina, deberá:
 - a) Verificar que el tratamiento que realice se encuentre reportado en el inventario respectivo. En caso contrario, deberá reportarlo con su superior jerárquico inmediato para su inclusión e identificación correspondiente.
 - b) Verificar de forma regular que el inventario que documenta el tratamiento que realiza, así como los avisos de privacidad respectivos, se encuentren actualizados.

- c) Observar en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
- d) Recabar el consentimiento para el tratamiento de los datos personales cuando proceda.
- e) Capacitarse de manera constante en materia de protección de datos personales.
- f) Reconocer sus obligaciones conforme al tipo de mando o encargo asignado, de la siguiente manera:

Tipo de mando	Obligaciones para el tratamiento de datos personales
Mandos superiores	a) Supervisar el tratamiento realizado, así como acercarse con las unidades especializadas en caso de considerar que las medidas de seguridad implementadas sean las necesarias para garantizar la integridad de los datos personales. b) Llevar el control de alta y baja de las personas servidoras públicas que puedan tener acceso a los datos personales en tratamiento.
Mandos medios	Coadyuvar en la actualización de registros de las personas servidoras públicas involucradas en el tratamiento; así como solicitar la cancelación de los permisos respectivos cuando una persona deje de laborar para la Oficina del Gobernador.
Nivel operativo	Conocer las medidas de seguridad que debe implementar al tratar datos personales y verificar qué medidas tomar en caso de vulnerar datos personales.

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

Consecuentemente con lo anterior, los órganos administrativos clasificaron los tipos de datos personales o documentación que cuente con los mismos, en niveles de protección de la siguiente forma: nivel estándar, nivel específico y nivel sensible.

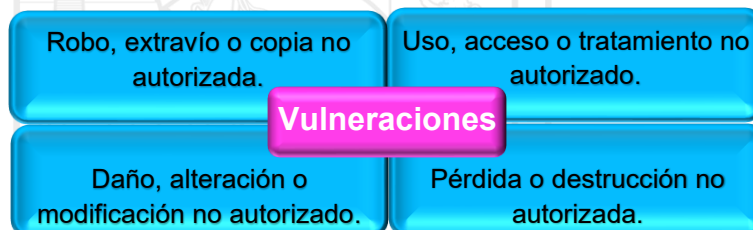
Dichos niveles se caracterizan, de manera enunciativa más no limitativa, con los ejemplos de información que contiene datos personales de la siguiente forma:

- a) **Nivel estándar:** Datos identificativos: datos contenidos en el acta de nacimiento, en la carta de aceptación de servicio social, edad, datos laborales, carrera, clave de elector, clave de empleado, Clave Única de Registro de Población (CURP), correo electrónico personal, currículum vitae, datos académicos (como grado escolar y constancia de estudios), estado civil, nombre de personas particulares, domicilios y números telefónicos de uso particular, datos de la pareja o familiares como dependientes económicos, etc.
- b) **Nivel específico:** aquellos datos personales que necesita necesariamente la autenticación de la persona titular de los mismos, tales como datos bancarios, contratos o pólizas, reporte de incidencias, préstamo o comodato por terceros, titular de la inversión, cuenta bancaria y otro tipo de valores, saldo insoluto, acreditación de personalidad en representación de menores de edad, adeudos/pasivos, bienes inmuebles, bienes muebles, circunstancias socioeconómicas, declaraciones tributarias, descuentos personales (ahorro voluntario, hipoteca, seguro médico, pensiones alimentarias, seguro de automóvil), fideicomisario, fideicomisos, fideicomitente, régimen matrimonial.
- c) **Nivel sensible:** tales como datos personales sensibles, por mencionar algunos: relativos a actividades de riesgo para la salud, adicciones, alergias, antecedentes e historial clínico, características biométricas de la palma de la mano, huella digital estampada o digitalizada, contraseñas de accesos a cuentas de carácter personal, creencias religiosas, filosóficas o morales, datos de salud pasado, presente y futuro, uso de medicamentos, hábitos de higiene, diagnósticos definitivos o preliminares de la salud, enfermedades familiares, tipo de sangre, temperatura corporal y discapacidades.

VI.- De las Vulnerabilidades

1. Se consideran posibles vulnerabilidades a la seguridad, dentro de las etapas de los tratamientos a datos personales en posesión de la Oficina, 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 diverso 32 de la Ley Estatal de Protección, se consideran vulneraciones de seguridad, en cualquier etapa de tratamiento de datos personales, las siguientes:



VII.- Inventario de Tratamientos y de Datos Personales de la Oficina

Conforme al artículo 29, fracción I 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 de la Oficina se detallará en el anexo 1 de este Documento, mismo que se podrá visualizar a la brevedad a través del sitio electrónico de la página web institucional del Poder Ejecutivo del Estado de Chiapas.

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

Inventario general de tratamientos por órganos administrativos	
Clave por OA	Denominación del órgano administrativo, con el listado de sus tratamientos identificados
02.A.1.I	Área de Recursos Humanos 1.- Para incapacidades médicas del personal de contrato y confianza. 2.- Para la integración y resguardo de expedientes personales. 3.- Para nómina de pago del personal. 4.- Para trámites de préstamos ante el Fideicomiso de Administración e Inversión “Fondo de Ahorro y Préstamos”. 5.- Para el Sistema de Control de Asistencia. 6.- Para el Sistema de Nóminas del Estado de Chiapas.
02.A.1.II	Área de Contabilidad y Recursos Financieros 1.- Para el pago de viáticos. 2.- Para la elaboración de órdenes de pago a proveedores.
02.A.1.III	Área de Recursos Materiales y Servicios Generales. 1.- Para la contratación adquisición, renta o compraventa de bienes y/o servicios. 2.- Para el manejo de información relacionada con proveedores y terceros.
02.A.1.IV	Área de Planeación 1.- Para la entrega de informes administrativos.
02.A.2	Unidad de Informática 1.- Para las cámaras de videovigilancia. 2.- Para habilitar el acceso a las áreas restringidas. 3.- Para la generación de la firma electrónica.
02.B	Dirección Jurídica 1.- Para el seguimiento de procedimientos jurisdiccionales y administrativos de cualquier nivel y autoridad.

Inventario general de tratamientos por órganos administrativos	
Clave por OA	Denominación del órgano administrativo, con el listado de sus tratamientos identificados
02.C	Coordinación de Asesores y Proyectos Estratégicos 1.- Para la atención y seguimiento de asesorías para el sector público y privado.
02.D	Coordinación de Giras, Logística, Ayudantía, Protocolo y Cultura Cívica 1.- Para el registro y control de asistencia del personal. 2.- Para incapacidades médicas del personal de contrato y confianza de la coordinación de giras. 3.- Para el trámite de pago de viáticos. 4.- Para la gestión y pago de tiempo extraordinario del personal de contrato. 5.- Para la integración del directorio telefónico del sector privado (h. Cuerpo diplomático, organismos internacionales). 6.- Para la integración del directorio telefónico del sector público (federal, estatal, municipal).
02.E.1	Dirección de Atención Ciudadana y Vinculación 1.- Para la recepción, atención y seguimiento de las peticiones realizadas al Gobernador. 2.- Para el registro de enlaces de atención y seguimiento de las peticiones realizadas al Gobernador.
02.E.2	Dirección de Información Pública 1.- Para capacitaciones, asesorías y/o cursos virtuales. 2.- Para la atención de solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales. 3.- Para brindar asesorías a través del módulo de transparencia y atención ciudadana. 4.- Para la atención y trámite de solicitudes para el ejercicio de derecho de acceso a la información pública. 5.- Para la atención y trámite de recursos de revisión o inconformidad en materia de acceso a la información pública. 6.- Para la atención y trámite de recursos de revisión en materia de datos personales.

Inventario general de tratamientos por órganos administrativos	
Clave por OA	Denominación del órgano administrativo, con el listado de sus tratamientos identificados
02.F.1	Coordinación General y de Administración 1.- Para el registro y control de asistencia del personal de la Representación del Gobierno del Estado de Chiapas en la Ciudad de México. 2.- Para incapacidades médicas del personal de la Representación del Gobierno del Estado de Chiapas en la Ciudad de México. 3.- Para el trámite de pago de viáticos del personal de Representación del Gobierno del Estado de Chiapas en la Ciudad de México. 4.- Para cámaras de videovigilancia de la Representación del Gobierno del Estado de Chiapas en la Ciudad de México.
02.F.2	Dirección de Asuntos Jurídicos y Enlace con Entes Públicos Federales 1.- Para el seguimiento de procedimientos jurisdiccionales y administrativos de cualquier nivel y autoridad. 2.- Para la asesoría y/o acompañamiento a personas chiapanecas que radiquen o se encuentren de visita en la Ciudad de México. 3.- Para la integración del directorio telefónico del sector público con los enlaces públicos federales ubicados en la Ciudad de México
02.G	Área de Archivos 1.- Para la organización, administración y conservación de archivos del Sistema Institucional de la Oficina del Gobernador.
02.H	Unidad de Enlace de Igualdad de Género 1.- Para capacitaciones, asesorías y/o cursos en modalidad presencial o virtual, impartidas a personas servidoras públicas en materia de género.

VIII.- Análisis de Riesgo y de Brecha

De conformidad con el artículo 29, fracción III de la Ley Estatal de Protección, el análisis de riesgo debe ser elaborado y actualizado 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 dispositivo 29, fracción IV 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 Estatal de Protección detalla la observancia de 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 el caso en particular, el hoy extinto 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., establecieron 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 íntegro 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, el cual los sujetos obligados deben observar y vigilar, los Análisis de Brecha y de Riesgo se detallan en los anexos números 2 y 3 del presente Documento de Seguridad, pero su contenido oficial será restringido y solo será dispuesto por los motivos anteriormente señalados.

Es dable hacer notar en el presente punto que, a la fecha de la actualización del presente Documento de Seguridad, no existe normatividad que se haya expedido por el nuevo Sistema Nacional de Acceso a la Información Pública o del Subsistema Estatal de Transparencia del Estado de Chiapas que se oponga o deje sin efectos la normatividad señalada en este apartado, lo que se encuentra sujeto a los ordenamientos que más adelante disponga el sistema o subsistema señalado en los que ocupe la observancia de este sujeto obligado.

Por otra parte, a través del sitio electrónico de Avisos de Privacidad dispuesto en la página web institucional de la Oficina, 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 de la Oficina.

IX.- Plan de Trabajo

Con fundamento en el artículo 29, fracción V de la Ley Estatal de Protección, se advierte la obligación de establecer y mantener las medidas de seguridad, bajo la elaboración de 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 administrativos y las fechas destinadas para la implementación de las medidas de seguridad nuevas o faltantes.

De tal forma, el Plan de Trabajo, detallado en el anexo número 4, 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 administrativos, conforme a las medidas de seguridad que se estiman faltantes, en el contexto de su propia organización interna y la evolución tecnológica de los sistemas y tratamientos de los datos personales.

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*, y dada la relevancia de restringir el acceso a la información, debidamente justificado mediante la sesión Sexta Sesión Extraordinaria del Comité de Transparencia de la Oficina del Gobernador del Estado de Chiapas, celebrada con fecha 25 de septiembre de 2026.

X.- Mecanismos de monitoreo y revisión

El artículo 24, fracción V de la Ley Estatal de Protección, establece 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 permita comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, el artículo 27, fracción VI de la Ley Estatal de Protección, establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, de ese mismo artículo y fracción de la Ley Estatal de Protección, dispone 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 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 aquellas 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 administrativos de la Oficina.

Para ello, los órganos administrativos, se auxiliarán en todo momento de la Unidad 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 a manera de medidas de seguridad que coadyuven en el avance y transversalización de la materia de protección de datos personales en el interior de la Oficina de Gobernador del Estado de Chiapas.

Respecto a los activos de carácter físico que se encuentren involucrados en las acciones de auditoría, monitoreo y revisión, la Coordinación Administrativa a través de la Unidad de Apoyo Administrativo instruirá al Área de Recursos Materiales y Servicios Generales, para que designe personal y auxilie dentro de las acciones señaladas, conforme al artículo 32 del Reglamento Interior de la Oficina de Gobernador del Estado de Chiapas.

Las instancias señaladas con antelación, darán cuenta de sus acciones a la Jefatura de Oficina de Gubernatura de manera oficial con copia a la Unidad de Transparencia, con efecto de su Superior conocimiento.

Asimismo, con la finalidad de observar el soporte documental y/o físico en los cuales se basan los tratamientos de datos personales, brindar asesoría técnica sobre operación de los archivos, y vigilar la aplicación de instrumentos archivísticos, la Jefatura de Oficina de Gubernatura podrá habilitar a personal del Área Coordinadora de Archivos, conforme al artículo 29, fracciones VI, XIII y XV de la Ley de Archivos del Estado de Chiapas.

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.**

En los términos como a continuación se desarrolla:

A. Mecanismo de monitoreo y supervisión.

Para establecer y mantener la seguridad de los datos personales, el artículo 47, fracción VII de la Ley Estatal de Protección, establece que se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están expuestos 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, el cual deberá ser desahogado por los órganos administrativos que, en el ámbito de sus atribuciones, sean las encargadas de los tratamientos 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:

Etapas	Objetivo	Ejecución	Documento final
Monitoreo	Registrar los controles de seguridad instaurados en determinado tratamiento.	Los órganos 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 administrativo.	Dictamen de Seguridad de los Datos Personales.

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

I. Etapa de Monitoreo

Se realizará tomando como punto de partida lo informado por cada órgano administrativo ante la Unidad de Transparencia en la integración del Documento de Seguridad, lo cual abarcó, 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, requerirá a cada órgano 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 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 administrativos se auxiliarán de la Unidad 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 administrativo del Reporte de Seguridad de Datos Personales se realizará de acuerdo con el calendario respectivo, mismo que será 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 5 de este documento.

II. Etapa de Supervisión

La persona Oficial de Protección de Datos Personales analizará los reportes de seguridad de datos personales remitidos por los órganos administrativos, 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, se 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 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 Unidad de Transparencia.

Si de las recomendaciones concluidas puede derivarse una estrategia que maximice la seguridad de los datos personales, se 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 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 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 6 de este documento.

B. Mecanismos de actuación ante alertas y vulneraciones.

El artículo 47, fracción VII de la Ley Estatal de Protección, dispone 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.

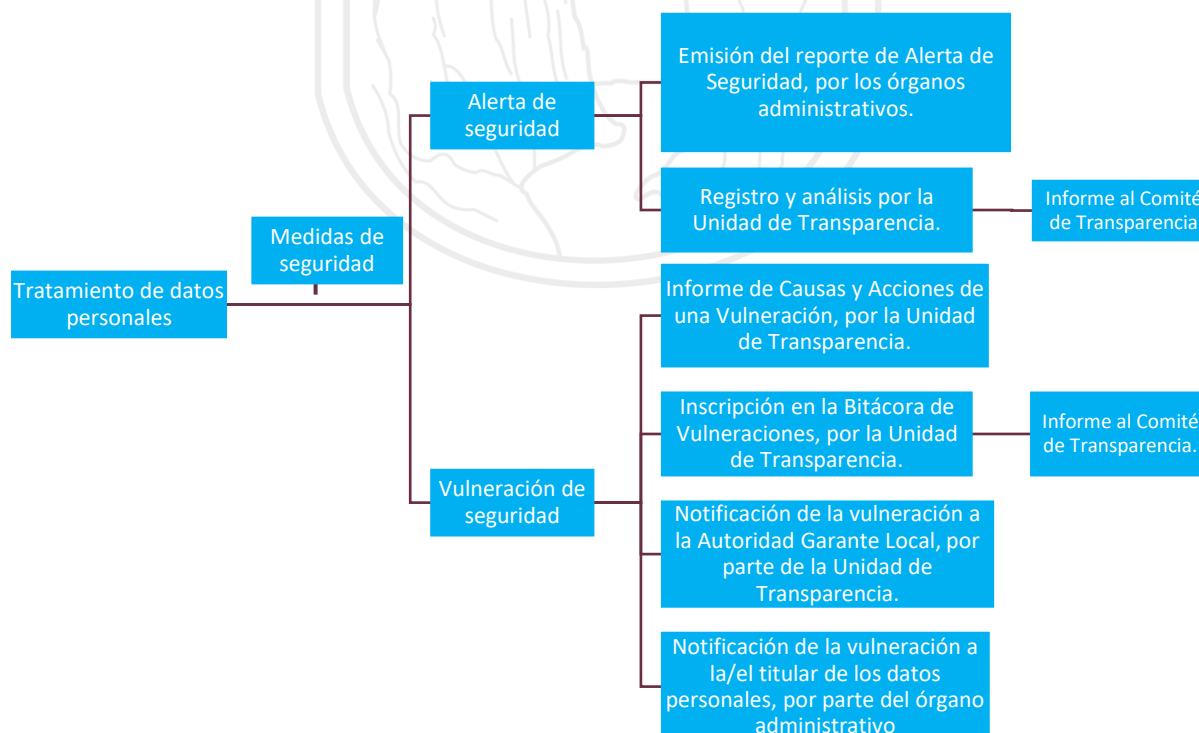
En ese sentido, el artículo 63, fracción VII de los Lineamientos Generales de Protección, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán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

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, la Unidad de Transparencia 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 auxiliará de la Unidad de Informática.

Bajo ese panorama, en este documento se definen los mecanismos que los órganos administrativos de la Oficina, a través de la Unidad de Transparencia, 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 de la Oficina, 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 administrativos de la Oficina 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 administrativos que en ejercicio de sus funciones realicen el tratamiento de datos personales.

El artículo 28 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 de la Oficina, 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 administrativos deberán verificar la materialización de los supuestos siguientes:

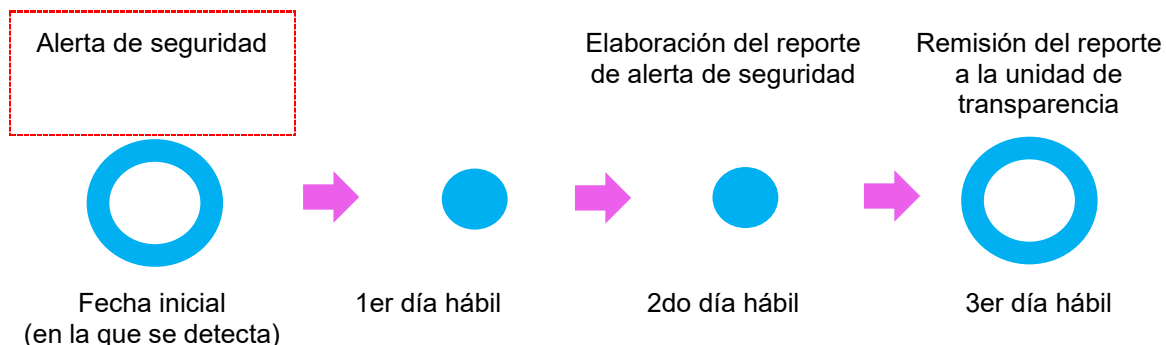
- Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.
- Que dichos efectos, de haberse materializado, hubieran representado un daño en las bases de datos, el hardware, software, archivos o documentos electrónicos o en papel, o en cualquier de los activos de importancia para cada órgano administrativo.

Para ello, los órganos administrativos, se auxiliarán de la Unidad 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:

- Al segundo día hábil siguiente a la fecha en que se detecte la amenaza, el órgano administrativo respectivo deberá elaborar un Reporte de Alerta de Seguridad, en los términos que más adelante se abordarán.
- Al tercer día hábil siguiente a la fecha en que se detecte la anomalía, el reporte deberá ser remitido a la Unidad de Transparencia quien efectuará el análisis correspondiente.

Si del análisis de la alerta de seguridad, la Unidad de Transparencia 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 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 administrativo.

Para establecer lo anterior, se requerirá el soporte técnico y administrativo de la Unidad de Informática, o en su caso al Área de Recursos Materiales y Servicios Generales con base en los artículos 32 y 34 del Reglamento Interior de la Oficina del Gobernador del Estado de Chiapas.

Verificada la existencia de una alerta de seguridad, el órgano 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 cuenta 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 cuenta 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 Unidad de Transparencia.

El formato del reporte de alerta de seguridad constituye el anexo 7 de este documento, al cual se le integrarán los informes que, en su caso, genere la Unidad de Informática y/o el Área de Recursos Materiales y Servicios Generales con base al soporte que brinde.

4. Registro y análisis de la alerta de seguridad.

Recibido el Reporte de Alerta de Seguridad, la Unidad de Transparencia 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 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 administrativos en las que la alerta de seguridad pueda desencadenarse.

Si del análisis de la alerta de seguridad, la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención, propondrá su integración en el Documento de Seguridad en el apartado respectivo, acorde a la autorización del Comité de Transparencia de la Oficina.

II. Vulneraciones de seguridad de los datos personales.

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

En primer término, de conformidad con lo establecido en el artículo 32 de la Ley Estatal de Protección, resulta indispensable que el órgano 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 administrativos de la Oficina.

Para ello, los órganos administrativos, se auxiliarán de la Unidad 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 31, 32, 33, 34 y 35 de la Ley Estatal de Protección, establecen las obligaciones siguientes:

- Analizar las causas por las cuales se presentó 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 las vulneraciones.
- Informar sin dilación alguna a la Autoridad Garante Local, 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 anteriores. 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 administrativo: día hábil siguiente a partir de la detección de la vulneración.
	Remisión del informe 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 administrativo respectivo.

Notificación a la Autoridad 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 administrativo, tendrá 72 horas a partir de que se detecte la vulneración.

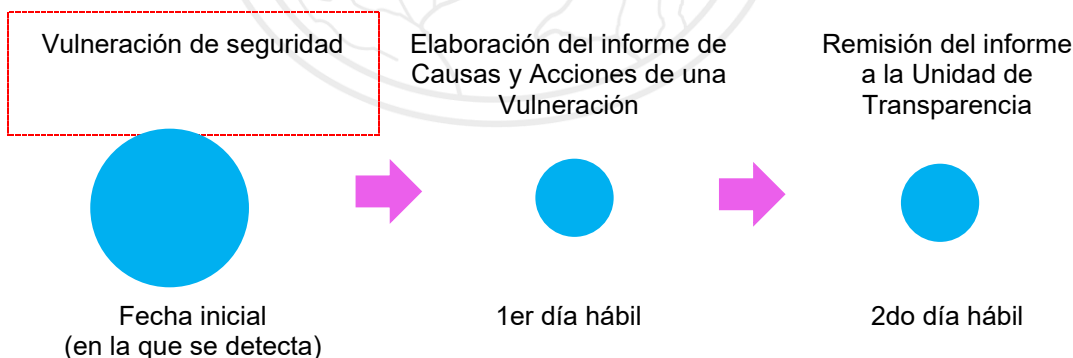
Lo cual, se detalla en los apartados siguientes.

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 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 de la Unidad 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 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 a la Oficina.

- ✓ 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. ▪ Decoror. ▪ 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 cuenta 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 con 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 puesto a través del cual pueda obtenerse más información respecto de 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 administrativo deberá remitir el informe a la Unidad de Transparencia, 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 de la Unidad de Informática.

El formato del referido informe constituye el anexo 8 de este documento.

Análisis de la vulneración de seguridad.

Recibido el Informe de Causas y Acciones de una Vulneración, la Unidad de Transparencia 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 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 en diversos tratamientos en los que la vulneración de seguridad pueda desencadenarse.

Si del análisis de la vulneración, la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención, hará la propuesta respectiva, y 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 33 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 la que ocurrió, su motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

En ese sentido, la Unidad de Transparencia la integrará en 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 administrativos de la Oficina; lo anterior, de conformidad con el formato que constituye el anexo 9 de este documento.

Por lo que, dentro del plazo de 24 horas siguientes al en que el órgano 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 administrativo, a efecto de que sea integrada a su bitácora interna de incidentes y vulneraciones a la seguridad.

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

El artículo 35 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 a la Autoridad Garante Local.

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 a la Autoridad Garante Local.
- B.** Verificar que el órgano 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 a la Autoridad 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 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 administrativo respectivo para restituir la seguridad del tratamiento de los datos personales.

Por ello, en términos de lo establecido en los artículos 54 y 55 de la Ley Estatal de Protección, en caso de que el órgano 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 a la Autoridad 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 a la Autoridad Garante Local.
- Cualquier otra información y documentación que se considere conveniente hacer del conocimiento de la Autoridad 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 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 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 administrativo el acuse de recibo o cédula de notificación correspondiente.

Sobre las auditorías en la materia.

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 24, fracción V de la Ley Estatal de Protección, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita 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, las actividades de auditoría se detallarán en una actualización del presente documento que, con base a los resultados de los otros mecanismos mencionados, se cuente con una justificación razonada para realizarse al interior.

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

El artículo 50, fracción XIX de la Ley Estatal de Protección, dispone 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 la Autoridad Garante Local, o a través de instituciones involucradas en la materia, y se lleven a cabo capacitaciones sobre los siguientes temas:

- **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.**

- Dirigido a todas las personas servidoras públicas de la Oficina.
- 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 la Oficina.
- 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 de la Oficina.

XII.- Actualización del Documento de Seguridad

Conforme al numeral 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 y Revisión 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 administrativos.
- Cuando se integre una política de seguridad de los datos personales en el Sistema de Gestión de Seguridad de la Oficina.
- Cuando los órganos administrativos lo soliciten en virtud de la maximización o perfeccionamiento de una medida de seguridad determinada.

La Unidad de Transparencia rendirá un informe cada año 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 de la Oficina del Gobernador, entrará en vigor al día siguiente de su aprobación por el Comité de Transparencia de la Oficina del Gobernador 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 de la Oficina del Gobernador del Estado de Chiapas resolverá lo conducente, conforme a los artículos 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Cuarta: Publíquese el presente Documento de Seguridad en la página electrónica de la Oficina del Gobernador del Estado de Chiapas.

Documento de Seguridad de la Oficina del Gobernador aprobado por los CC. Javier Abarca Arias, Director Jurídico, Víctor Hugo Alegría Cordero, Responsable de la Unidad de Transparencia, José Eduardo Alabath Paniagua, Coordinador Administrativo, Josselin López García, Directora de Atención Ciudadana y Vinculación y Francisco Javier Bermúdez Núñez, Responsable del Área de Archivos, en calidad de Presidente y Secretario Técnico, el primero y el segundo de los nombrados y los demás en calidad de vocales, personas servidoras públicas integrantes del Comité de Transparencia de la Oficina del Gobernador, a través de la Sexta Sesión Extraordinaria, celebrada con fecha 25 del mes de septiembre del año 2026 dos mil veintiséis. Rúbricas -