MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES

Anexo I

Documento de seguridad

ÍNDICE

Presentación 01
Marco normativo 02
Abreviaturas y denominaciones 03
Deber de seguridad 03
Obligatoriedad del Documento de Seguridad 04
Medidas de seguridad de los datos personales de la CEDH 05
Obligaciones en materia de tecnologías de la información 07
Hábitos en materia de seguridad 14
Integración del Documento se Seguridad 15
Definición de funciones y obligaciones de los servidores públicos involucrados 17
Inventario de datos personales y sistemas 18
Análisis de riesgo 19
Análisis de brecha 23
Plan de trabajo 24
Mecanismos de monitoreo, revisión, alertas, vulneraciones y auditoría 24
A. Mecanismos de monitoreo y supervisión de la protección de datos personales 26
I. Etapas de monitoreo 27
II. Etapas de Supervisión 28
B. Mecanismos de actuación ante alertas y vulneraciones a la seguridad de los datos personales 29
I. Alertas de seguridad de los datos personales 31
II. Vulneraciones de seguridad de los datos personales 34
C. Mecanismos de auditoría en materia de datos personales 42
I. Finalidades y objetivos 43
II. Instancia ejecutora del programa y ámbito de aplicación 44
III. Etapas de las auditorías en materia de datos personales 44
Programa de capacitación en materia de datos personales 50
Actualización del documento de seguridad 51

PRESENTACIÓN

De conformidad con el artículo 3, fracción XIV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, un Documento de Seguridad es el 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.

El artículo 35 de dicha legislación, establece que los sujetos obligados deberán elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de sus sistemas de tratamiento.
II. Las funciones y obligaciones de las personas que traten datos personales.
III. El análisis de riesgos.
IV. El análisis de brecha.
V. El plan de trabajo.
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
VII. El programa general de capacitación.

En cumplimiento al marco normativo se procedió a la elaboración del presente instrumento, incluyendo en principio, referencias básicas respecto de la protección de los datos personales, a través de los capítulos siguientes:

- ✓ Marco Normativo.
- ✓ Deber de seguridad.
- ✓ Obligatoriedad del Documento de Seguridad.

Posteriormente, se describieron de manera general las medidas de seguridad técnicas, físicas y administrativas que se mantienen en el CEDH:

- ✓ · Medidas de seguridad en el CEDH.
- ✓ Obligaciones en materia de tecnologías de la información.
- ✓ Hábitos en materia de seguridad.

Asimismo, se puntualizó la forma en que se documentaron y estudiaron el inventario de datos personales y sistemas, la definición de funciones y obligaciones de los servidores públicos involucrados en el tratamiento de datos personales, los análisis de riesgo y brecha y el plan de trabajo respectivo; lo anterior, a través de los capítulos siguientes:

- ✓ Integración del Documento de Seguridad.
- ✓ Inventario de datos personales y sistemas.
- ✓ Definición de funciones y obligaciones de los servidores públicos involucrados.
- ✓ Análisis de riesgo.
- ✓ Análisis de brecha.
- ✓ Plan de trabajo.

Adicionalmente, se establecieron los mecanismos que serán operados para el monitoreo, revisión y auditoría de las medidas de seguridad, a través de los capítulos siguientes:

- ✓ · Mecanismos de monitoreo, revisión, alertas, vulneraciones y auditoría.

A continuación, se definió el programa de capacitación en materia de protección de datos personales a través del capítulo y anexo respectivo.

Finalmente, se describieron los supuestos de actualización del presente documento.

ABREVIATURAS Y DENOMINACIONES

CEDH: Comisión Estatal de los Derechos Humanos

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

ITAIPCH: Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

Ley Estatal: Ley de Protección de Datos Personales en Posesión de Sujetos Obliga- dos del Estado de Chiapas.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Publico, publicados en el Diario Oficial de la Federación el 26 enero de 2018.

Lineamientos para la Evaluación de Impacto: Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, publicados en el Diario Oficial de la Federación el 23 de enero de 2018.

Lineamientos para la Portabilidad: Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicado en el Diario Oficial de la Federación el 12 de febrero de 2018.

Unidades administrativas: Las áreas administrativas que integran el Comisión Estatal de los Derechos Humanos.

MARCO NORMATIVO

Respecto a la Protección de Datos Personales al interior de la Comisión Estatal de los Derechos Humanos – Chiapas, resulta aplicable el siguiente marco normativo:

1.- LEY FEDERAL:

- ✓ Constitución Política de los Estados Unidos Mexicanos.

  Artículo 1, párrafo segundo y tercero, de la (Denominación del Capítulo reformada DOF 10-06-2011, publicado en el Diario Oficial de la Federación de Última reforma publicada el 22 de marzo de 2024)
- ✓ Ley General de Transparencia y Acceso a la Información Pública.
- ✓ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- ✓ Lineamientos Generales de Protección de Datos Personales para el sector público.

2.- LEY ESTATAL:

- ✓ Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.
- ✓ Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

3.- NORMATIVIDAD INTERNA DE LA COMISIÓN ESTATAL DE LOS DERECHOS HUMANOS

- ✓ Reglamento Interior de la Comisión Estatal de los Derechos Humanos, vigente.

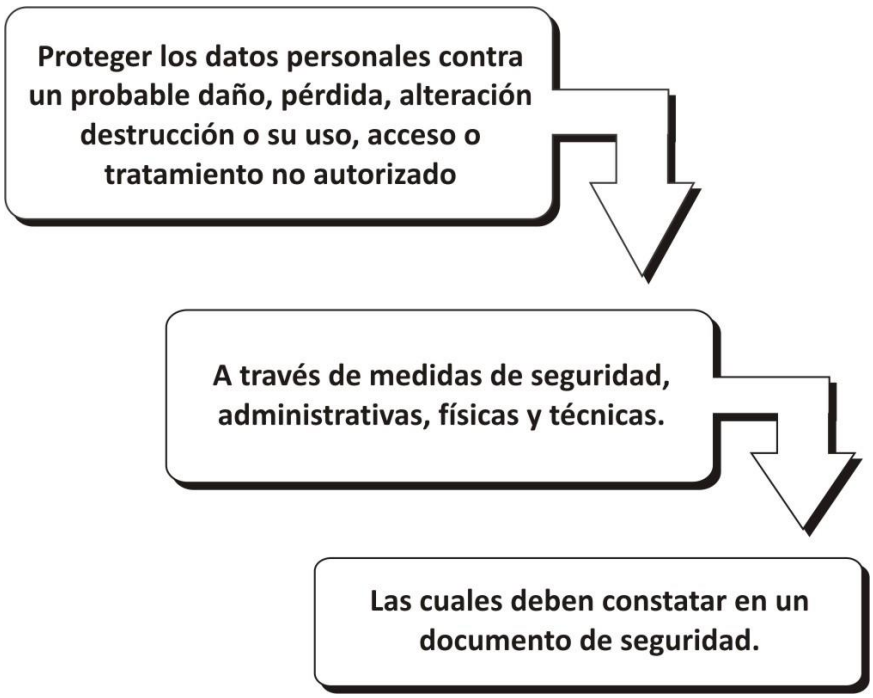
DEBER DE SEGURIDAD

El artículo 31 de la Ley General 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 responsable de la Comisión Estatal de los Derechos Humanos 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 trata- miento no autorizado.
- ✓ Garantizar su confidencialidad, integridad y disponibilidad.

En ese sentido, el artículo 35 de la Ley General, dispone 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 l CEDH debe realizar lo siguiente:



Esto con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

OBLIGATORIEDAD DEL DOCUMENTO DE SEGURIDAD

En el ámbito de sus respectivas competencias y bajo el marco normativo referido, las disposiciones expuestas en este documento resultan de observancia obligatoria para las áreas que realicen el tratamiento de datos personales.

La Unidad de Transparencia se encuentra a disposición de los servidores públicos de la CEDH, para brindar la orientación necesaria en relación con el presente documento, la cual podrá solicitarse:

- ✓ Vía correo electrónico: transparencia@cedhchiapas.org.mx.

- ✓ Vía telefónica: Conmutador 961-60 28980; 961 60 28981, extensión 265.
- ✓ Vía presencial: 1 Sur Oriente, esquina 2ª Calle Oriente Sur S/N, Edificio Plaza 4º Piso Barrio San Roque, Tuxtla Gutiérrez, Chiapas, código postal 29000.

MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES EN LA CEDH

Las medidas de seguridad de los datos personales, son el conjunto de acciones, actividades, controles o mecanismos que permiten protegerlos contra su daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, garantizando con ello su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad pueden clasificarse en administrativas, físicas y técnicas, las cuales de conformidad con el artículo 3, fracciones XXI, XXII y XXIII, de la LGPDPPSO, y 5, fracciones XXV, XXVI y XXVII, de la LPDPPSOCH, se refieren a lo siguiente:

1. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal;

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

   a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

   b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

   c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,

   d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

3. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos

personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se consideran las actividades siguientes:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y,

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

El esquema anterior se reflejó en el formulario de Examinación de riesgo, donde las áreas declararon los controles y medidas de seguridad que mantienen para la protección de los datos personales de cada tratamiento.

Analizando dichas declaraciones, en conjunto con las acciones y mecanismos que la CEDH mantiene para asegurar su función y el cumplimiento de sus atribuciones; se procede a enunciar, de manera general, las medidas de seguridad de los datos personales.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

1. Estructura orgánica y organigrama general de las áreas administrativas de la CEDH;

2. Programa General de Capacitación en Materia de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual concentra los objetivos, ejes temáticos y programas que deberán implementarse para el cumplimiento de las atribuciones y principios relacionados con la capacitación y actualización de los servidores públicos de la CEDH en las materias indicadas; y

3. Las establecidas para el cumplimiento de los principios, deberes y políticas de protección de datos personales en el Sistema de Gestión de Seguridad de Datos Personales y Programa General de Datos Personales.

MEDIDAS DE SEGURIDAD FÍSICAS

1. Las estipuladas por los servidores públicos 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; y
- ✓ El acceso a los datos personales condicionado al personal autorizado.

MEDIAS DE SEGURIDAD TÉCNICAS

1. Las estipuladas por la Unidad Técnica de Servicios Informáticos, para impulsar la operación eficiente y la modernización en la automatización de los procesos necesarios para el ejercicio de las funciones de la Comisión Estatal de los Derechos Humanos , a través de la generación de sistemas y administración de la infraestructura de cómputo;

2. Las estipuladas por los servidores públicos 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 cada servidor público con acceso autorizado;
   - ✓ Contraseña única para el acceso a los datos personales.

OBLIGACIONES EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN

En la CEDH implementará Políticas Generales en Materia de Tecnologías de la Información y Comunicaciones, mismas que resultan de observancia obligatoria para todas las instancias, así como para usuarios externos que usen sus recursos y servicios informáticos.

En ese contexto, resulta relevante referir las políticas que se relacionaran directamente con la seguridad de los datos personales.

CUIDADO Y USO DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS

El usuario deberá abstenerse de:

- ✓ Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad de la CEDH sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red.

- ✓ Exponer las redes de la CEDH a cualquier tipo de amenaza interna y/o externa.

LA UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS DEBERÁ:

- ✓ Supervisar que sólo aquellos equipos propiedad de la CEDH, sean sujetos a los programas de mantenimiento preventivo, correctivo e instalación de software institucional.

- ✓ Auxiliar a las instancias competentes para la realización de inspecciones o supervisión del uso de los bienes informáticos, así como de la información contenida en estos.

ASIGNACIÓN DE BIENES INFORMÁTICOS

El usuario deberá:

- ✓ Asumir la responsabilidad total del resguardo y uso que se le dé a los bienes informáticos.

USO DEL SOFTWARE INSTITUCIONAL

El Usuario deberá:

- ✓ Utilizar el software institucional bajo su resguardo, únicamente para la realización de sus funciones y conforme a la licencia de uso, por lo que no deberá distribuirlo o reutilizarlo en un equipo distinto al asignado para el desempeño de sus funciones.

El usuario deberá abstenerse de:

- ✓ Instalar cualquier software adicional (comercial, shareware, freeware, etcétera) al originalmente preinstalado en los equipos de cómputo, sin previa autorización de la Unidad Técnica de Servicios Informáticos;

- ✓ Alterar el software institucional instalado en los equipos de cómputo propiedad de la CEDH.

CONTROL DE VIRUS

El usuario deberá:

- ✓ Hacer caso omiso y eliminar los correos electrónicos no deseados o de personas desconocidas, cadenas de correos y evitar su reenvío, previendo la propagación de virus, páginas de suplantación de identidad (phishing) u otro tipo de software malicioso;

- ✓ Previo a su ejecución analizar con el software antivirus todos aquellos medios como, discos compactos, DVD, memorias USB u otros tipos de almacenamiento externos al equipo de cómputo, que sean conectados a este; y

- ✓ Levantar el reporte correspondiente, si se sospecha de alguna infección por virus en algún equipo de cómputo.

El usuario deberá abstenerse de:

- ✓ Introducir software malicioso en el equipo de cómputo, así como herramientas que realicen conexiones desconocidas o túneles, las cuales pueden provocar un daño a la red o información de la CEDH, con amenazas como virus, worms, spyware, ráfagas de correo electrónico no solicitado, o cualquier otro tipo de malware.

- ✓ Modificar la configuración del software antivirus y de seguridad en los equipos de cómputo, sin la autorización de la Unidad Técnica de Servicios Informáticos.

INFORMACIÓN GENERADA O CONTENIDA EN LOS EQUIPOS DE CÓMPUTO

El usuario deberá:

- ✓ Asumir que toda la información generada, recibida, archivada, enviada o comunicada mediante el uso de cualquiera de los recursos o servicios informáticos que le fueron suministrados para el ejercicio propio de su cargo, es del dominio de la CEDH y por ende susceptible de supervisión en cualquier momento por las instancias competentes con el auxilio de la Unidad Técnica de Servicios Informáticos;

- ✓ Realizar periódicamente copias de seguridad de la información bajo su resguardo, relativa a las funciones que desempeña, a fin de evitar pérdidas causadas por algún daño en el equipo;

- ✓ Entregar todos los archivos y documentos digitales que contengan información de dominio de la CEDH, al momento de cambiar de adscripción o separarse de la institución;

- ✓ Verificar que, al crear un recurso compartido en la red, únicamente se concedan los permisos a usuarios específicos;

- ✓ Asumir la responsabilidad de la información que genera y comparte mediante los recursos de la red, definiendo los permisos de lectura o escritura correspondientes; y,

- ✓ Bloquear el equipo de cómputo, al momento de ausentarse del lugar de trabajo.

El usuario deberá abstenerse de:

- ✓ Extraer información propiedad de la CEDH, para fines diversos a las funciones

encomendadas;

- ✓ Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad de la CEDH sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red;

- ✓ Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la Comisión Estatal de los Derechos Humanos de Chiapas; y,

- ✓ En caso de requerir asesoría con relación a cualquiera de los puntos anteriores, se deberá de solicitar a la Unidad de Informática.

La Unidad Técnica de Servicios Informáticos deberá:

- ✓ Proporcionar, a solicitud del usuario, asesoría para realizar copias de seguridad de la información que resida en el equipo de cómputo; y,

- ✓ Revisar que todas las computadoras de escritorio y portátiles propiedad de la CEDH, tengan configurado un protector de pantalla con contraseña, el cual se active transcurrido el tiempo de inactividad que determine la propia área.

ASIGNACIÓN DE CUENTAS DE USUARIO Y CONTRASEÑAS

- ✓ Las cuentas de usuario, contraseñas de acceso a la red y sistemas de información son de carácter personal e intransferible; y,

- ✓ Las cuentas de usuario creadas y/o utilizadas en el software institucional son propiedad de la CEDH.

El usuario deberá:

- ✓ Responsabilizarse del resguardo, confidencialidad y uso que se les dé a sus cuentas de usuario, contraseñas de acceso a la red y sistemas de información.

- ✓ Firmar el resguardo que para tales efectos elabore la Unidad de Informática, relacionado con la custodia y asignación de la cuenta de usuario y contraseña provisional; será su responsabilidad cambiar esta contraseña para acceder a los servicios de red la primera

vez que haga uso del servicio.

El usuario deberá abstenerse de:

- ✓ Evadir o modificar los mecanismos de autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario; y,
- ✓ Usar y/o divulgar contraseñas ajenas.

La Unidad Técnica de Servicios Informáticos deberá:

Establecer la conformación y vigencia de las contraseñas para los servicios de red, de acuerdo con lo siguiente:

- ✓ Al menos ocho caracteres;
- ✓ Incluir al menos un número;
- ✓ Incluir al menos una mayúscula y una minúscula;
- ✓ Incluir al menos un carácter especial;
- ✓ No se podrán utilizar ninguna de las cinco contraseñas registradas previamente; y,
- ✓ La vigencia de la contraseña será de 90 días naturales.

USO DE CORREO ELECTRÓNICO

El usuario deberá:

- ✓ Establecer comunicación con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado;
- ✓ Privilegiar el uso del correo electrónico institucional sobre los servicios de correo electrónico personal, para el intercambio de información oficial, a través de las cuentas oficiales asignadas para ello;
- ✓ Asumir la responsabilidad del contenido de los mensajes enviados con su cuenta institucional de correo electrónico;
- ✓ Considerar que las cuentas de correo personales institucionales son intransferibles, y están asociadas exclusivamente a un usuario;
- ✓ Realizar periódicamente copias de seguridad de los mensajes de correo electrónico (buzón de correo electrónico y archivo de datos de Webmail), a fin de evitar pérdidas

causadas por algún daño en el equipo;

- ✓ Entregar los correos electrónicos (preferentemente en archivo de datos de Webmail) que contengan información del dominio de la CEDH, al momento de cambiar de adscripción o separarse de la institución; y,

- ✓ Permitir en todo momento a las unidades administrativas, en el ámbito de sus atribuciones el acceso a la información contenida en la cuenta de correo electrónico proporcionada por la CEDH.

El usuario deberá abstenerse de:

- ✓ Enviar mensajes institucionales, a través de servicios de correo electrónico personal; la realización de esta actividad quedará bajo la estricta responsabilidad del usuario;

- ✓ Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad de la CEDH, sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red; y,

- ✓ Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función del Comisión Estatal de los Derechos Humanos de Chiapas.

El Titular del área administrativa deberá:

- ✓ Asumir la responsabilidad del contenido de los mensajes enviados con la cuenta institucional de correo electrónico oficial del órgano jurisdiccional o del área administrativa.

La Unidad Técnica de Servicios Informáticos deberá:

Administrar los servicios de correo electrónico, para ello podrá definir, el aspecto siguiente:

- ✓ En caso de que el usuario necesite recuperar un archivo que ha sido bloqueado por el sistema o enviar un archivo no permitido por el tipo o tamaño, deberá comunicarse con la Unidad de Informática para su análisis y atención.

MENSAJERÍA INSTANTÁNEA INSTITUCIONAL

El usuario deberá:

- ✓ Establecer comunicación con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado;
- ✓ Asumir la responsabilidad del contenido de los mensajes enviados con su cuenta de mensajería instantánea institucional, esto incluye entre otros: contenido de material ofensivo u obsceno, cualquier quebrantamiento de propiedad intelectual, derechos de autor o cualquier información que pueda constituir el objeto de un ilícito y/o de responsabilidad administrativa; y,
- ✓ Considerar que las cuentas institucionales personales son intransferibles, y están asociadas exclusivamente a un solo usuario, quien será responsable del uso que se dé a su cuenta.

El usuario deberá abstenerse de:

- ✓ Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad de la CEDH sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red; y,
- ✓ Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la Comisión Estatal de los Derechos Humanos de Chiapas.

INTERNET

El usuario deberá:

- ✓ Observar que el acceso a los servicios de Internet por medio de la red de la CEDH, sea a través de los recursos informáticos destinados y aprobados para tal fin por la Unidad de Informática; y,
- ✓ Solicitar a la Unidad de Informática, el acceso a Internet para los equipos de cómputo y dispositivos externos de la CEDH, para su evaluación, y en su caso, aprobación y

configuración, a través de los medios de conexión destinados para dicho fin, con el objeto de evitar riesgos.

El usuario deberá abstenerse de:

- ✓ Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada propiedad de la CEDH sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a los servidores públicos de sus funciones o que comprometa los bienes informáticos y los servicios de red;

- ✓ Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función del Poder Judicial de la Federación; y,

- ✓ Utilizar cuentas con el nombre, las siglas, el logo o identificaciones oficiales de la CEDH en redes sociales, blogs y sitios de Internet, que lo ostenten como portavoz de comunicados oficiales u opiniones institucionales hacia Internet. El área responsable de la imagen y comunicación institucional de la CEDH, es la única que podrá atender o responder peticiones de información institucional que se emitan en redes sociales.

HÁBITOS EN MATERIA DE SEGURIDAD

Al realizar el tratamiento de datos personales, los servidores públicos deberán habituarse a la realización de lo siguiente:

- ✓ Mantener el área de trabajo sin documentos importantes y/o dispositivos de almacenamiento electrónico a la vista;

- ✓ Cerrar los cajones y resguardar la información personal bajo su custodia;

- ✓ Evitar dejar los documentos que ya no sean utilizados sobre impresoras, escáneres o copiadoras;

- ✓ Realizar la eliminación segura de información en equipos de cómputo, celulares, tabletas y medios de almacenamiento electrónico;

- ✓ Fijar periodos para la retención y destrucción de la información personal que se maneja;

- ✓ Fomentar una cultura de la seguridad de la información;
- ✓ Realizar respaldos periódicos de los datos personales;
- ✓ Utilizar cerraduras y candados para resguardar los datos personales;
- ✓ Bloquear o suspender la sesión en equipos de cómputo y dispositivos móviles cuando dejas de usarlos; y,
- ✓ Validar el destinatario de una comunicación antes de realizarla.

INTEGRACIÓN DEL DOCUMENTO DE SEGURIDAD

El artículo 33, de la LGPDPPSO y 47, de la LPDPPSOCH, establece la elaboración del documento de seguridad, el cual se debe integrar con los elementos siguientes:

Para dicha integración, el numeral en cita dispone que el documento de seguridad sea elaborado, entre otros elementos, con la información que cada una de las áreas de la CEDH proporcionen. En atención a ello, para constituir el presente instrumento la Unidad de Transparencia siguió la metodología siguiente:

1. Proporcionar a las áreas que realizan el tratamiento de datos personales lo siguiente:

- ✓ Nociones del derecho a la protección de datos personales y los deberes de las áreas de la Comisión Estatal de los Derechos Humanos; y,

- ✓ Pasos que seguir para la realización del listado de funciones y obligaciones de los servidores públicos involucrados, inventario de datos, análisis de riesgo, análisis de brecha y plan de trabajo.

Se requirió la elaboración de los listados de funciones y obligaciones de los servidores públicos que intervienen en cada uno de los tratamientos que realizan, así como su respectivo inventario de los datos personales y sistemas, análisis de riesgo y de brecha.

2. Desahogado lo anterior, se integró por cada área el Inventario de Datos Personales y Sistemas, las Funciones y Obligaciones, el Análisis de Riesgo, el Análisis de Brecha respectivo.

3. Una vez que se analizó la información obtenida, se formularon los mecanismos siguientes:

- ✓ Monitoreo y Supervisión en la Protección de los Datos Personales;

- ✓ Actuación ante Alertas y Vulneraciones a la Seguridad de los Datos Personales;

- ✓ De Auditoría en Materia de Datos Personales, y,

- ✓ Se creó un Programa de Capacitación que, entre otros objetivos, cubriera los aspectos inherentes al Documento de Seguridad.

4. Todo lo anterior, fue integrado en el presente documento, el cual será sometido a aprobación del Comité de Transparencia, quien de conformidad con el artículo 83, segundo párrafo y 84, fracciones I, V y VII, de la LGPDPPSO, 113 y 114, fracciones I, VI y VIII, de la LPDPPSOCH; es la autoridad máxima en materia de protección de datos personales, contando con las atribuciones de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales; supervisar, en coordinación con las instancias competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad; así como establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

DEFINICIÓN DE FUNCIONES Y OBLIGACIONES DE LOS SERVIDORES PÚBLICOS INVOLUCRADOS

El artículo 33, fracción II, de la LGPDPPSO, 47, fracción II, de la LPDPPSOCH, disponen que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá definir las funciones y obligaciones del personal involucrado en su tratamiento.

Tal actuación, se desarrolla con fundamento en el artículo 57, de los Lineamientos Generales, al estipular que los responsables deberán establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales.

Con el objeto de realizar lo anterior, conforme a sus respectivas competencias, se requirió a las instancias para que realizaran las acciones siguientes:

Identificar

- ✓ La totalidad de las operaciones que se realicen con datos personales.

Ordenar

- ✓ Las operaciones en relación con la forma en que se efectúan, ya sea manuales o automatizadas.

Relacionar

- ✓ Cada operación con el servidor público a su cargo, señalando desde el ejecutor hasta el responsable.

Exponer

- ✓ De cada servidor público, las funciones que realiza de acuerdo al Manual Específico, y las funciones que realiza en la operación del tratamiento.

Para documentar lo anterior, las áreas integraron cada una de las actividades que integran el tratamiento de datos personales efectuado, los aspectos siguientes:

I. Nombre de la actividad;

II. Forma de obtención de los datos personales;

III. Descripción de la actividad;

IV. Nombre y cargo del servidor público responsable de la actividad;

V. Funciones del servidor público;

VI. Función que realiza el servidor público responsable en el desarrollo de la actividad;

VII. Nombre y cargo del servidor público ejecutor de la actividad;

VIII. Funciones del servidor público;

IX. Función que realiza el servidor público ejecutor en el desarrollo de la actividad; y,

X. Nombre y cargo del servidor público que almacena los archivos de la actividad.

INVENTARIO DE DATOS PERSONALES Y SISTEMAS

El artículo 33, fracción III, de la LGPDPPSO, 47, fracción III, de la LPDPPSOCH, establecen como una de las actividades interrelacionadas con el establecimiento y mantenimiento de las medidas de seguridad de los datos personales, la realización de un inventario de datos personales y de los sistemas de tratamiento.

El artículo 58, de los Lineamientos Generales, estipula que dicho inventario deberá elaborarse con la información básica de cada tratamiento de datos personales, considerando, al menos, los elementos siguientes:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;

II. Las finalidades de cada tratamiento de datos personales;

III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;

IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable; y,

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

En ese sentido, con el objeto de establecer y mantener las medidas de seguridad para la protección de los datos personales, los titulares de las áreas que con motivo del ejercicio de sus funciones cuenten con uno o varios sistemas de datos, deberán informarlo a la Unidad de

Transparencia, a efecto de que sea integrado al inventario de datos personales y sistemas.

Bajo ese esquema, atendiendo a lo estipulado en el artículo 58, de los Lineamientos Generales, las áreas competentes declararon la información concerniente a los sistemas de datos personales con que cuentan, lo cual se encuentra documentado a través de los archivos electrónicos denominados Inventario de Datos Personales y Sistemas.

ANALIS DE RIESGO

De conformidad con el artículo 33, fracción IV, de la LGPDPPSO, 47, fracción IV, de la LPDPPSOCH, 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.

De conformidad con lo estipulado en el artículo 60, de los Lineamientos Generales, en la realización del análisis de riesgo se deberá considerar lo siguiente:

- ✓ La existencia de requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico para proteger los datos personales;
- ✓ El valor de los datos personales de acuerdo con su clasificación previamente definida, y su ciclo de vida, de conformidad con la normatividad aplicable; y,
- ✓ El valor y exposición de los activos involucrados en su tratamiento.

Un activo es la información, el conocimiento sobre los procesos, el personal, *hardware, software* y cualquier otro recurso involucrado en el tratamiento de datos personales que tenga valor para la CEDH.

Existen dos tipos de activos, los primarios y de soporte.

Los activos primarios corresponden a los procesos de gestión y actividades, así como a la información crítica, por ejemplo, toda la información vital para la operación de la CEDH, la información personal especificada dentro del marco regula- torio de privacidad e información estratégica.

Los activos de soporte son aquellos que apoyan a los activos primarios para su operación y consisten en: Equipo de cómputo (hardware), aplicaciones (software), equipos de

comunicaciones, personal, instalaciones y estructura organizacional.

- ✓ Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y,

- ✓ El riesgo inherente a los datos personales tratados, su sensibilidad (datos personales sensibles), el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión; siempre en función y estricto apego a la normatividad aplicable.

En cumplimiento a ello, las áreas de la CEDH analizaron el riego existente en cada uno de los tratamientos de datos personales que realizan, describiendo los aspectos siguientes:

I. Información general

a) La identificación de los datos personales que se obtienen o reciben; y,

b) Motivo por el cual se recaban o reciben los datos personales.

II. Finalidades del tratamiento

a) La denominación del tratamiento de datos personales que realiza y la forma en que se opera, detallando el fundamento legal y normativo aplicable al tratamiento;

b) La categoría correspondiente a los datos personales tratados, es decir, si se ejerce sobre datos de carácter identificativo, de características personales, circunstancias sociales, datos académicos y profesionales, detalles del empleo, de información comercial, datos económicos o financieros y de seguro;

c) La duración del tratamiento que realiza, es decir, si es instantáneo, o si tiene un periodo de duración de días, semanas, meses, años, o resulta de tiempo indeterminado;

d) Si la obtención de los datos tiene como finalidad la supervisión o evaluación sistemática y exhaustiva de aspectos personales, como son, aquellos a través de los cuales se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc., de personas identificadas o identificables;

e) Si la obtención de los datos tiene como finalidad el tratamiento de datos personales sensibles;

f) Si la finalidad del tratamiento pudiera cumplirse recabando un menor número de datos personales;

g) Si la finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad;

h) Si el tratamiento de los datos personales tiene la finalidad de elaborar documentos, perfiles o es utilizado para la toma de decisiones;

i) Si el número de servidores públicos involucrados en el tratamiento de datos personales resulta insuficiente, suficiente o excesivo; y,

j) Identificar si servidores públicos adscritos a otras áreas se encuentran involucra- dos en el tratamiento de datos personales; refiriendo las áreas, la forma en que se desenvuelve su participación en el tratamiento de datos personales y si se considera que tal intervención es necesaria.

III. Tecnologías empleadas para el tratamiento

a) La tecnología implementada en el tratamiento de datos personales, describiendo el nombre y el modo de empleo.

IV. Transferencia de datos personales

a) Si en el tratamiento de datos personales se realiza una transferencia de datos, destacando la normatividad correspondiente y el instrumento legal en el que se convino dicha transferencia; y,

b) Si en el tratamiento de datos personales se realiza una transferencia de datos a entidades internacionales, señalando la normatividad correspondiente, el nombre y país de la entidad internacional y describa el instrumento legal en el que se convino dicha transferencia.

V. Controles existentes

a) Respecto de los controles que se encuentran instaurados para la protección de los datos personales, se identificó el nombre del control, su objetivo, la forma en que se instrumenta, el nombre y cargo de los servidores públicos involucrados en la ejecución del control, el documento en que se registra la existencia del control destacando el nombre y cargo del servidor público responsable, así como los resultados y demás cuestiones inherentes a su elaboración;

b) Identificación de la naturaleza de los controles existentes, es decir, de carácter preventivo o correctivo;

c) Controles ejecutados en los casos en que el tratamiento de datos personales se encuentre documentado en papel;

d) Controles ejecutados en los casos en que el tratamiento de datos personales sea documentado de forma electrónica; y,

e) La efectividad de los controles implementados para garantizar la seguridad de los datos personales.

VI. Percepción de la existencia de un riesgo

a) Previa reflexión de los controles implementados, consideración relativa a si el tratamiento de datos personales puede conllevar una pérdida o alteración de la información;

b) Si los controles y medidas de seguridad existentes para la obtención, tratamiento, resguardo y archivo de los datos personales cumplen su objetivo de manera efectiva;

c) Si los riesgos considerados pueden afectar los controles y medidas de seguridad implementadas en el tratamiento de datos personales;

d) La forma en la que los riesgos señalados pueden reducirse a futuro;

e) Si los riesgos identificados pueden ser compartidos con otra instancia; y,

f) Si las formas de reducir los riesgos identificados pueden ser compartidas con otra instancia.

En el análisis del riesgo declarado por las áreas, se consideraron los factores siguientes:

- ✓ La categoría correspondiente a los datos personales tratados;
- ✓ La duración del tratamiento que realiza;
- ✓ Si la obtención de los datos tiene como finalidad la supervisión o evaluación sistemática y exhaustiva de aspectos personales;
- ✓ Si la obtención de los datos tiene como finalidad el tratamiento de datos personales sensibles;
- ✓ Si la finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad;
- ✓ Si el tratamiento de los datos personales tiene la finalidad de elaborar documentos, perfiles o es utilizado para la toma de decisiones; y,
- ✓ Si en el tratamiento se realiza una transferencia de datos personales.

Con la información obtenida, la Unidad de Transparencia integró por cada área el análisis de riesgo respectivo, realizando con ello el estudio del nivel de riesgo latente.

ANALIS DE BRECHA

El artículo 33, fracción V, de la LGPDPPSO, 47, fracción V, de la LPDPPSOCH; estipulan que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, es necesaria la elaboración de un análisis de brecha en el que se comparen las medidas de seguridad existentes contra las faltantes.

EL artículo 61, de los Lineamientos Generales, dispone que en la realización del análisis de brecha se debe considerar lo siguiente:

- ✓ Las medidas de seguridad existentes y efectivas;
- ✓ Las medidas de seguridad faltantes; y,
- ✓ La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

De modo que, una vez identificados los riesgos y medidas de seguridad ineludibles, es procedente el análisis de brecha, en el que se identifiquen los controles que deben ser implementados.

Bajo tales directrices, partiendo de los “controles existentes” y de la “percepción de la existencia de un riesgo”, las áreas competentes analizaron las brechas atendibles justificando los aspectos siguientes:

- ✓ Si los controles de seguridad declarados han resultado efectivos para garantizar la seguridad de los datos personales;
- ✓ Si después del análisis de los controles de seguridad, se considera que el trata- miento de datos personales puede conllevar una pérdida o alteración de la información;
- ✓ Si los controles y medidas de seguridad existentes para la obtención, tratamiento, resguardo y archivo de los datos personales cumplen su objetivo de manera efectiva;
- ✓ Los riesgos que se consideran pueden afectar los controles y medidas de seguridad implementadas en el tratamiento de datos personales; y,
- ✓ La forma en la que se estima que los riesgos señalados pueden reducirse a futuro.

En congruencia con lo anterior, identificaron expresamente la brecha atendible respectiva al tratamiento de datos personales realizado.

PLAN DE TRABAJO

El artículo 33, fracción VI, de la LGPDPPSO, 47, fracción VI, de la LPDPPSOCH, estipula que, para establecer y mantener las medidas de seguridad, se deberá 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.

El artículo 62, de los Lineamientos Generales, dispone que el Plan de Trabajo debe definir las acciones a implementar de acuerdo con el resultado del análisis de riesgo y brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, considerando los recursos designados, el personal interno de la instancia y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Así, el Plan de Trabajo concentra los retos que en materia de seguridad de datos personales afrontan las áreas competentes, sustentado en el análisis de los riesgos y las medidas de seguridad que se estiman deben implementarse, en el contexto de su propia organización interna y la evolución tecnológica de sus sistemas.

Al respecto, y relacionando el riesgo localizado y la brecha atendible, de cada tratamiento de datos personales las áreas establecerán lo siguiente:

1. El mecanismo de control para atender la brecha identificada;
2. El periodo de monitoreo;
3. La fecha en que se implementará; y,
4. Evidencia entregable.

MECANISMOS DE MONITOREO, REVISIÓN, ALERTAS, VULNERACIONES Y AUDITORÍA

El artículo 30, fracción V, de la LGPDPPSO, 44, fracción V, de la LPDPPSOCH, 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 permita comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, el artículo 35, fracción VI, de la LGPDPPSO, 50, XVIII, de la LPDPPSOCH, establecen que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, el numeral 33, fracción VII, de la LGPDPPSO, 47, fracción VII, de la LPDPPSOCH, disponen que se deba de monitorear y revisar de manera periódica los aspectos siguientes:

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

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, 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:

1. 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);

2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas;

4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo; y,

7. Los incidentes y vulneraciones de seguridad ocurridos.

Además de lo expuesto, el artículo referido estipula que el responsable deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

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; y,

C. Mecanismo de Auditoría en Materia de Datos Personales.

A. Mecanismo de monitoreo y supervisión en la protección de datos personales. Para establecer y mantener la seguridad de los datos personales, el artículo 33, fracción VII, de la LGPDPPSO, 47, fracción VII, LPDPPSOCH, 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 el área administrativa 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 del Reporte de Seguridad de Datos Personales, el cual deberá ser desahogado por las áreas 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 o requerimientos que se consideren pertinentes.

El proceso anterior, se describe de la forma siguiente:

ETAPA	OBJETIVO	EJECUCIÓN	DOCUMENTO FINAL
Monitoreo	Registrar los controles de seguridad instaurados en determinado tratamiento.	Las instancias 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 la instancia respectiva.	Dictamen de Seguridad de los Datos Personales.

A continuación, se describe cada una de las etapas.

I. ETAPA DE MONITOREO

Se realizará tomando como punto de partida lo informado por cada área ante la Unidad de Transparencia, en la integración del Documento de Seguridad, lo cual abarcó, entre otros aspectos, lo siguiente:

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

En vista de lo anterior, la Unidad de Transparencia requerirá a cada área, 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.

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; y,

   - ✓ 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 área 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.

II. ETAPA DE SUPERVISIÓN

La Unidad de Transparencia analizará los reportes de seguridad de datos personales remitidos por las áreas, verificando especialmente lo siguiente:

1. La idoneidad y efectividad de las medidas de seguridad y control respecto del tratamiento;

2. La suficiencia de controles preventivos y correctivos;

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

4. Avances generados conforme a lo establecido en el Plan de Trabajo; y,

5. 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 plasmaran las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad.

Lo que será notificado a las áreas, 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, la Unidad de Transparencia la integrará en el Plan de Trabajo de la CEDH, con el objeto de que sean atendibles por aquellas instancias que les puedan resultar aplicables.

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 diversas instancias, la Unidad de Transparencia deberá analizar la necesidad de actualizar el Documento de Seguridad, en términos de lo establecido para esos efectos.

B. MECANISMOS DE ACTUACIÓN ANTE ALERTAS Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

El artículo 33, fracción VII, de la Ley General, 47, fracción VII, de la Ley Estatal, 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, 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.

Por lo que, 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 podrá auxiliar de la Unidad Técnica de Servicios Informáticos.

Bajo ese panorama, se definen los mecanismos que las áreas de la CEDH, 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, resulta elemental distinguir entre una alerta y una vulneración de seguridad. La diferencia entre ambos conceptos, se exponen de la forma siguiente:

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 de un 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 autor- izado; y, 4. El daño, la alteración o modificación no autorizada.
No implica la materialización de una vulneración.	Implica un daño a los activos de la CEDH, como 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 los titulares de los datos personales.

Dichos mecanismos, deberán desarrollarse, como se representa a continuación:

<table>
<tr><td rowspan="6">Tratamiento de datos personales</td><td rowspan="6">Medidas de seguridad</td><td rowspan="2">Alerta de seguridad</td><td>Emisión del reporte de Alerta de Seguridad, por las instancias</td><td rowspan="2">Informe al Comité de Transparencia</td></tr>
<tr><td>Registro y análisis por la Unidad de Transparencia</td></tr>
<tr><td rowspan="4">Vulneraciones de seguridad</td><td>Informe de Causas y Acciones de una Vulneración por las instancias.</td><td rowspan="4">Informe al Comité de Transparencia</td></tr>
<tr><td>Inscripción en la Bitácora de Vulneraciones, por la Unidad de Transparencia.</td></tr>
<tr><td>Notificación de la Vulneración al ITAIPCH, por parte de la Unidad de Transparencia.</td></tr>
<tr><td>Notificación de la vulneración al particular, por parte del área.</td></tr>
</table>

Establecido lo anterior, se procede a exponer el mecanismo que las instancias de la CEDH deberán efectuar cuando:

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

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 SEGURIDAD DE LOS DATOS PERSONALES.

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

El artículo 31 de la LGPDPPSO, 45 de la LPDPPSOCH, estipulan 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, dispone que dichas medidas constituye 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, a efecto de maximizar la protección de los datos personales en posesión de la CEDH, 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; y,
- ✓ Integrar las estrategias de prevención en el Plan de Trabajo a efecto de que, en los casos conducentes, se implementen como medidas adicionales de seguridad.

Es importante destacar, que resultará indispensable identificar que efectivamente los hechos acaecidos constituyan una alerta a la seguridad de los datos personales, para lo cual, las áreas 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; y,

- ✓ 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 la instancia.

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 área respectiva 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 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 Plan de Trabajo.

Lo que precede, se representa de la forma siguiente:

Alerta de seguridad		**Elaboración del reporte de Alerta de Seguridad**	**Envió del reporte de Alerta de Seguridad da la Unidad de Transparencia**
Fecha en la que se detecta	**Día hábil 1**	**Día hábil 2**	**Día hábil 3**

REPORTE DE ALERTA DE SEGURIDAD

Una vez que la instancia advirtió un 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 siguientes supuestos:

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

- ✓ 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 la instancia.

Verificada la existencia de una alerta de seguridad, el área deberá emitir un Reporte de Alerta de Seguridad, en el cual se deberá considerar, como mínimo, el desarrollo de los aspectos siguientes:

a) Detección.
    1. Nombre, cargo y adscripción del servidor público que detectó la amenaza;
    2. Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta;
    3. Tratamiento o sistema en que ocurrió;
    4. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema; y,
    5. Datos personales involucrados en la amenaza.

b) Proyección de una posible vulneración.
    1. Elementos que permitieron el desarrollo o persistencia de la amenaza;
    2. Elementos que contuvieron el desarrollo o persistencia de la amenaza;
    3. Actuaciones que pueden evitar la reincidencia de la amenaza; y,
    4. Descripción de los efectos que hubiera causado la anomalía si hubiere persistido hasta materializar una vulneración.

c) Medidas de seguridad involucradas
    1. Descripción clara de los controles físicos o electrónicos involucrados en la amenaza;
    2. Circunstancias que, individual o conjuntamente, permitieron la existencia de la amenaza;
    3. 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;
    4. 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; y,
    5. 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.

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 contener los aspectos siguientes:

a) El impacto que tiene la alerta en la seguridad de los datos personales;

b) Observaciones en materia de seguridad que el área debe observar en el futuro desarrollo del tratamiento;

c) Medidas de seguridad adicionales que se estime conducente implementar; y,

d) Si resulta posible determinar una estrategia de prevención con instancias 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, procederá a su integración en el Plan de Trabajo de la CEDH.

II. VULNERACIONES DE SEGURIDAD DE LOS DATOS PERSONALES.

El mecanismo que aquí se describe, resulta obligatorio para las áreas 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 LGPDPPSO, 52, de la LPDPPSOCH, resulta indispensable que la instancia identifique que efectivamente los hechos acaecidos 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; y,
  4. El daño, la alteración o modificación no autorizada.
- ✓ 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 de los activos de importancia para las áreas de la CEDH.

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 al 41 de la LGPDPPSO, 54 al 58 de la LPDPPSOCH, establecen las obligaciones siguientes:

1. Analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar que la vulneración se repita;

2. Inscribir la vulneración en la bitácora de las vulneraciones; y,

3. Informar sin dilación alguna al titular y al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Chiapas (ITAIPCH), las vulneraciones que afecten de forma significativa derechos patrimoniales o morales, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

A continuación, se describe 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 área: 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 área respectiva.
Notificación al ITAIPCH	✓ La Unidad de Transparencia tendrá 72 horas a partir de que se detecte la vulneración.
Notificación al particular afectado	✓ El área tendrá 72 horas a partir de que se detecte la vulneración.

Lo cual, se precisa a detalle 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 realizar lo siguiente:

1. Dentro del día hábil siguiente a la fecha en que se detecte, el área respectiva deberá elaborar un *Informe de Causas y Acciones de una Vulneración*, en los términos que más adelante se abordarán; y,

2. Al segundo día hábil siguiente a la fecha en que se detecte, el área 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:

Vulneración de seguridad	**Elaboración del Informe de Causas y Acciones**	**Envío del informe a la Unidad de Transparencia**
Fecha en la que se detecta	**Día hábil 1**	**Día hábil 2**

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 siguientes aspectos:

1. **Información general de la vulneración.**

   a) **Detección**

      I. Nombre, cargo y adscripción del servidor público que detectó la vulneración;

      II. Fecha, hora y lugar en que se detectó la vulneración;

      III. Tratamiento o sistema que fue vulnerado;

      IV. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema;

      V. Datos personales involucrados en la vulneración; y,

VI. Descripción detallada de la forma en que se detectó la vulneración.

b) Investigación

I. Fecha y hora en que se inició la investigación de la vulneración;

II. Nombre y cargo del servidor público designado para la investigación de la vulneración;

III. Naturaleza de la vulneración;

IV. Fecha y hora de la vulneración;

V. Descripción detallada de la forma en que se desarrolló la vulneración;

VI. Descripción detallada de las afectaciones que fueron materializadas;

VII. Tipo y número aproximado de titulares afectados; y,

VIII. Posibles consecuencias de la vulneración.

c) Medidas de seguridad vulneradas e impacto causado

I. Descripción clara de cada uno de los controles físicos o electrónicos que operan en el tratamiento o sistema, incluyendo el servidor público responsable de su implementación;

II. Identificación de la totalidad de las personas que cuentan con acceso a cualquiera de las fases del tratamiento, incluyendo servidores públicos o personas ajenas al CEDH;

III. Identificación y descripción de la vulneración materializada; y

IV. Determinación del nivel de impacto causado por la vulneración en relación con el tratamiento o sistema (alto, medio, bajo), considerando el número de titulares afectados, así como el tipo y naturaleza de los datos personales involucrados en la vulneración.

V. Determinación relativa a si la vulneración generó una afectación significativa a los derechos patrimoniales y/o morales de los titulares de los datos personales.

De conformidad con lo previsto en los Párrafos Tercero y Cuarto del artículo 66, de los Lineamientos Generales, para determinar la existencia de una afectación significativa patrimonial

o moral, se deberán atender los criterios siguientes:

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 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 titular.

2. **Acciones preventivas y correctivas.**

a) 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 que efectivamente hubiera podido llevar a cabo tal prevención;

b) Si la vulneración no puso ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo;

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

d) Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración;

e) Recomendaciones para el titular afectado;

f) Medio puesto a través del cual pueda obtenerse mayor información respecto de la vulneración;

g) Datos de contacto de los servidores públicos designados para la gestión de la vulneración; y,

h) 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 área deberá remitir el informe a la Unidad de Transparencia, quien efectuará el registro y análisis correspondiente.

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 explicar los aspectos siguientes:

a) El impacto que tiene la vulneración de seguridad en la protección de los datos personales;

b) Observaciones en materia de seguridad que la instancia debe observar en el futuro desarrollo del tratamiento;

c) Medidas de seguridad adicionales que se estime conducente implementar; y,

d) 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 procederá a su integración en el Plan de Trabajo de la CEDH.

Inscripción en la bitácora de vulneraciones

De conformidad con el artículo 39, de la LGPDPPSO, 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 integrará la Bitácora de Vulneraciones a la Seguridad de los Datos Personales, en la que se concentrarán las vulneraciones acaecidas en la totalidad de las áreas de la CEDH.

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

Informe de la vulneración al ITAIPCH y al titular de los datos personales

El artículo 40, de la LGPDPPSO, 54, de la LPDPPSOCH, dispone que, ante una vulneración que afecte de forma significativa derechos patrimoniales o morales, se deba informar sin dilación alguna al titular y al ITAIPCH.

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 los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Al respecto, el artículo 66, de los Lineamientos Generales, estipula que la notificación del informe al 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.

Ocurrida una vulneración, la Unidad de Transparencia deberá realizar lo siguiente:

A. Notificar la vulneración al ITAIPCH; y,

B. Verificar que el área respectiva notifique al particular o particulares afectados por la vulneración identificada.

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

Notificación de la vulneración al ITAIPCH

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

1. Identificará si en el Informe de Causas y Acciones de una Vulneración, el área respectiva consideró que la afectación sufrida causaba un daño significativo patrimonial o moral en detrimento de los titulares de los datos personales afectados; y,

2. Supervisará las acciones implementadas por la instancia 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 LGPDPPSO, 54 y 55, de la LPDPPSOCH, en caso de que la instancia 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 ITAIPCH que, de conformidad con el artículo 67, de los Lineamientos Generales, 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 titulares afectados;
- ✓ 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 al titular;
- ✓ El medio puesto a disposición del 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 ITAIPCH; y,
- ✓ Cualquier otra información y documentación que se considere conveniente hacer del conocimiento del ITAIPCH.

Notificación de la vulneración a los particulares

De haberse considerado la actualización de una afectación significativa al patrimonio o a la moral del titular o titulares de los datos personales, la instancia respectiva deberá realizar un informe que considere los aspectos siguientes:

- ✓ La naturaleza de la vulneración;
- ✓ Los datos personales comprometidos;
- ✓ Las recomendaciones al 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; y,
- ✓ Cualquier otra información y documentación que se considere conveniente para apoyar a los titulares de los datos personales afectados.

La Unidad de Transparencia podrá auxiliar al área en la elaboración del informe, el cual deberá notificarse por el área respectiva al particular o los particulares afecta- dos 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 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.

Hecho lo anterior, el área deberá remitir a la Unidad Administrativa el acuse de recibo respectivo.

C. MECANISMO DE AUDITORÍA EN MATERIA DE DATOS PERSONALES

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la LGPDPPSO, 44, fracción V, de la LPDPPSOCH, que establecen, 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, párrafo tercero de los Lineamientos Generales, 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 Plan de Trabajo;
- ✓ Prevenir la materialización de vulneraciones a la seguridad de los datos personales; y,
- ✓ 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 principal 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; y,
4. Precisar el proceso a través del cual se seleccionarán las instancias auditables.

Es importante referir que el alcance que tendrán las auditorías practicadas, se concentrará exclusivamente en el análisis de la forma en que cada área, 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 a la CEDH perfeccionar el manejo y protección de los datos personales.

II. Área ejecutora del programa y ámbito de aplicación

Respecto de la ejecución del Programa, de conformidad con el artículo 30, fracción V, de la LGPDPPSO, 44, fracción V, de la LPDPPSOCH, 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 las áreas que en ejercicio de sus funciones realicen el tratamiento de datos personales, serán los sujetos auditables materia del programa, 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.

La etapa de apertura tendrá la finalidad de definir el personal del área auditada 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 la instancia 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 Programa de Protección de Datos Personales y el Documento de Seguridad.

En la etapa conclusiva, la Unidad de Transparencia puntualizará a la instancia auditada 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 las instancias 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 de manera oficial al área correspondiente, lo siguiente:

1. La fecha en que dará inicio la auditoría, la cual deberá realizarse con un mínimo de 5 días hábiles entre la notificación del documento y su celebración;

2. La necesidad de que el área auditada designe al personal con el que la Unidad de Transparencia substanciará la auditoría; y,

3. 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 área auditada.

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, deberá elaborar una minuta en la que se precisará el desarrollo de la propia reunión, la cual deberá ser firmada por los involucrados.

Acuerdo de inicio

En el día estipulado para el comienzo de la auditoría, la Unidad de Transparencia emitirá un acuerdo de inicio en el que deberá asentar lo siguiente:

a) El día en que comenzará y finalizará la auditoría;

b) El servidor público designado por la Unidad de Transparencia para sustanciar la auditoría;

c) El servidor público designado por el área auditada para sustanciar la auditoría;

d) Identificación del tratamiento o tratamientos de datos personales materia de la auditoría;

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

f) La documentación, sistema o espacio físico que deberá estar plenamente disponible para ser examinado; y,

g) Los datos de contacto de la Unidad de Transparencia, ante los cuales podrán solventarse dudas relacionadas con el desarrollo de la auditoría.

El acuerdo de inicio deberá ser notificado al área respectiva 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 las áreas 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 estipulado 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 área auditada;

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 área auditada;

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, el área auditada deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales;

E. **Principio de calidad**: Que el área auditada 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 área auditada 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 área auditada haya informado al titular, a través del aviso de privacidad, la existencia y características principales del trata- miento al que serán sometidos sus datos personales;

H. **Principio de responsabilidad**: Que el área auditada haya adoptado la políticas y mecanismos necesarios para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General, Ley Estatal y Lineamientos Generales, que establecen las disposiciones en materia de protección de datos personales;

I. **Deber de seguridad**: Que el área auditada haya establecido y mantenido medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión; y,

J. **Deber de confidencialidad**: El área auditada 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:

1. La estimación de cumplimiento correspondiente a cada principio y deber;

2. Consideraciones que se estimen relevantes en cuanto al tratamiento de los datos personales;

3. Recomendaciones en materia de seguridad de los datos personales;

4. 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 las instancias deberán remitir las evidencias respectivas a la Unidad de Transparencia; y,

5. Conclusiones generales de la auditoría.

c) Etapa conclusiva

Reunión final

La Unidad de Transparencia convocará al área auditada 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 el área deberá remitir las evidencias correspondientes.

Efectuada la reunión final, la referida Unidad elaborará una minuta en la que se concentrarán las conclusiones alcanzadas, la cual deberá ser signada por los involucrados.

Cumplimiento de observaciones y requerimientos

Dentro del plazo otorgado en el documento de conclusiones, el área auditada 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 del examen, la Unidad de Transparencia, corrobora que han sido adecuadamente cumplidos 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 área auditada debe demostrar su acatamiento.

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 área auditada a más tardar dentro de los tres días hábiles siguientes a su emisión.

Selección de las instancias auditables

La programación de las auditorías se realizará a través de una selección de instancias basada en criterios aplicados al panorama general que guarda el tratamiento de los datos personales en la CEDH.

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 áreas involucradas en el tratamiento de datos personales;
- ✓ El número de tratamientos que cada área 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;
  - Información comercial;
  - Datos económicos; y,
  - Financieros y de seguro.
- ✓ Áreas que operen uno o varios tratamientos que conlleven datos personales sensibles.

Criterios de selección

Atendiendo a los objetivos de este programa, los criterios de selección serán los siguientes:

1. Tratamientos con un número considerable de riesgos;
2. Tratamientos que, de ser objeto de una vulneración, tengan como consecuencia un impacto mayor al titular de los datos personales;
3. 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 de la CEDH;
4. Instancias cuyas funciones impliquen un alto número de tratamientos; y,
5. Instancias 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; y,
- ✓ 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

Una vez realizada la selección de las instancias bajo los criterios expuestos, la Unidad de Transparencia ponderará la cronología que deberá seguir la calendarización de las auditorías, lo cual deberá hacerse del conocimiento del Comité de Transparencia para su aprobación.

PROGRAMA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

El artículo 33, fracción VIII, de la LGPDPPSO, 47, fracción VIII, de la LPDPPSOCH, 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.

El numeral 64, de los Lineamientos Generales, señala que se deberán diseñar e implementar programas a corto, mediano y largo plazo, que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

Lo anterior, considerando lo siguiente:

a) Los requerimientos y actualizaciones del sistema de gestión;

b) La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

c) Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales; y,

d) Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

En ese sentido, a propuesta de la Unidad de Transparencia, en coordinación con el Comité deberá aprobar anualmente el programa de capacitación de datos personales, mismo que se integrará a este documento.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El artículo 36, de la LGPDPPSO, 51, de la LPDPPSOCH, establecen que los sujetos obligados deberán actualizar el documento de seguridad cuando ocurra alguno de los eventos siguientes:

Cambio en el nivel de riesgo	**Ante modificaciones sustanciales al tratamiento que deriven en un cambio en el nivel de riesgo.**
Mejora continua	**Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.**
Mitigación del efecto de una vulneración.	**Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.**
Incluir acciones correctivas y preventivas	**Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.**

En razón 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 ha 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 diversas instancias.
- ✓ - Cuando se integre una política de seguridad de los datos personales en el Sistema de Gestión de Datos Personales de la CEDH.
- ✓ Cuando las instancias lo soliciten en virtud de la maximización o perfecciona- miento de una medida de seguridad determinada.

La Unidad de Transparencia deberá rendir un informe anual al Comité de Transparencia que detalle si hubo o no actualizaciones al Documento de Seguridad.

UNID AD DE TRANSP ARENCIA
CEDH CHIAPAS