
# POLÍTICAS INTERNAS Y MEDIDAS PREVENTIVAS PARA LA GESTIÓN, TRATAMIENTO Y PROTECCIÓN DE LOS DATOS PERSONALES EN LA CEDHV

Edición 2023

SGS 2024-2025

COMISIÓN ESTATAL DE DERECHOS HUMANOS VERACRUZ

# Contenido

# 1. PRESENTACIÓN

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.

De acuerdo con la Ley 316 de Protección de Datos Personales para el Estado de Veracruz de Ignacio de la Llave, los sujetos obligados deben establecer las Políticas Internas que rijan la actuación de los servidores públicos involucrados en el tratamiento de los datos personales que posean en cumplimiento de sus atribuciones.

Este documento recopila los principios, deberes, derechos, obligaciones y responsabilidades que tienen las personas titulares, así como las y los servidores públicos y/o encargados respecto al tratamiento de los datos personales a los cuales tienen acceso en ejercicio de sus funciones. Con su aplicación, se busca garantizar la protección de los datos de las personas que solicitan la intervención o colaboran con esta Comisión en el cumplimiento de sus atribuciones.

Asimismo, las presentes políticas establecen las medidas mínimas de carácter físico, técnico y administrativo, así como las acciones de respuesta a posibles vulneraciones que las áreas responsables de los Sistemas de Protección de Datos de la CEDH y aquellas que por sus atribuciones intervienen en su tratamiento, deben implementar para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión de este Organismo.

Las disposiciones señaladas en el presente documento, fueron retomadas de la normatividad local y nacional existente en materia de protección de datos personales, así como de diversos instrumentos internacionales relacionados con la materia, con el objetivo de estandarizar y conformar una guía de actuación para las y los servidores públicos de esta Comisión en el tratamiento de los datos personales, que conforman la parte normativa.

Asimismo, el presente documento, contiene un apartado en el que se enlistan las medidas de seguridad o controles que deben implementarse en cada ámbito de amenazas detectadas dentro del Organismo, como parte de la actualización del Sistema de Gestión de Seguridad para la protección de datos personales que se implementará durante el periodo 2024-2025.

# I. NORMATIVIDAD

## Objetivo, fundamento y ámbito de validez

### 1. Objetivo

Las presentes Políticas Internas y Medidas Preventivas tienen por objeto establecer las obligaciones, deberes, responsabilidades y en general las acciones y buenas prácticas que las y los servidores públicos de la Comisión Estatal de Derechos Humanos Veracruz, así como las o los encargados de los datos personales de ésta, deben observar a la luz de los preceptos de la Ley 316 de Protección de Datos Personales en Posesión de los Sujetos Obligados.

### 2. Fundamento Legal

Los preceptos aquí contenidos deberán sujetarse a las disposiciones de la Ley 316 de Protección de Datos Personales en Posesión de los Sujetos Obligados, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y los Lineamientos que para tales efectos emita el Sistema Nacional de Transparencia o en su caso el Instituto Veracruzano de Acceso a la Información Pública y Protección de Datos Personales.

### 3. Ámbito de validez

Las políticas internas y medidas preventivas serán de aplicación obligatoria para las y los servidores públicos de la Comisión Estatal de Derechos Humanos del Estado de Veracruz que como parte de sus atribuciones conferidas en el Reglamento Interno y/o en los Manuales de Organización o Procedimientos, obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan de datos personales, y deberán observarse por las y los Encargados de los Datos de la CEDHV.

## Disposiciones Generales

### 4. Definiciones

Además de los Términos establecidos en el Artículo 3 de la Ley, para efectos de las presentes Políticas Internas y Medidas Preventivas, se entenderá por:

**Activos:** Las bases de datos, sistemas o expedientes que contengan datos personales, recabados o en posesión de la CEDH con motivo de sus atribuciones. Ejemplo: base de datos de las solicitudes de intervención, expedientes de quejas, de recursos humanos o de prestadores de servicio social, declaraciones patrimoniales y de intereses de servidores públicos o diagnósticos realizados, etc.

**Alerta de seguridad:** Hecho o evento que se detecta y/o registra en los sistemas de tratamiento físico o electrónico, el cual advierte de un posible incidente de seguridad.

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

**Bases de datos**: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

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

**Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

**Encargado (a):** Toda persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

**Instituto:** Instituto Veracruzano de Acceso a la Información Pública y Protección de Datos Personales.

**Ley o Ley 316:** Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave.

**Responsable:** Cualquier autoridad, dependencia, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del

Estado, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

Supresión: La baja archivística de los datos personales conforme a la normativa aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular: La persona física a quien corresponden los datos personales.

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

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

Vulneración: Aquel accidente, siniestro, incidente u otro que materialice una brecha de seguridad (afectación a datos de carácter personal), que puede tener un origen accidental o intencionado, ya sea que afecte datos o bases físicas o automatizadas (digitales) tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

## 5. Derechos de los Titulares de los Datos Personales (Derechos ARCO)

En todo momento la persona Titular de los datos o su representante podrán solicitar a los Servidores Públicos de la CEDH el acceso, rectificación, cancelación y oposición de los datos personales que le conciernen. El ejercicio de cualquiera de los derechos ARCO no es requisito previo ni impide el ejercicio de otro.

Para efectos de lo anterior, de acuerdo con la Ley, por derechos ARCO deberá entenderse lo siguiente:

5.1 Acceso: La persona Titular tiene derecho a acceder a sus datos que obren en posesión de la CEDH, así como a conocer toda la información relacionada con las condiciones y generalidades de su tratamiento.

5.2 Rectificación o corrección: La persona Titular tiene derecho a solicitar la corrección de sus datos en posesión de la CEDH cuando éstos sean inexactos, incompletos o estén desactualizados.

5.3 Cancelación: La persona Titular tiene derecho a solicitar a la CEDH la cancelación de sus datos de los archivos, registros, expedientes y sistemas en los que obre, a fin de que los mismos dejen de ser tratados por personal de este Organismo y ya no estén en posesión del mismo.

5.4 Oposición: La persona Titular podrá oponerse al tratamiento de sus datos personales o exigir que cese cuando dicho tratamiento pueda causar un daño o perjuicio al titular; o produzca efectos jurídicos no deseados o afecta de manera significativa sus intereses.

Para la procedencia de los derechos de cancelación u oposición deberá analizarse la viabilidad del ejercicio del derecho, atendiendo a las circunstancias del caso concreto.

## 6. Obligaciones de los Responsables y Encargados

Las y los servidores públicos de la CEDH que participen en el tratamiento de datos personales de acuerdo con las atribuciones de su área de adscripción deberán:

- Conocer y en su caso, poner a la vista de los titulares el Aviso de Privacidad que le corresponda al área de su adscripción.
- Conocer e informar a los titulares de la existencia del Sistema de Protección que corresponda al área de su adscripción.
- Facilitar el ejercicio de los derechos ARCO a los titulares que lo soliciten.
- Cumplir con las medidas de seguridad físicas, administrativas o técnicas necesarias para el correcto tratamiento de los datos personales establecidas en su área de adscripción.
- Cumplir en todo momento con los deberes de seguridad y confidencialidad de los datos personales.
- Apegar su actuar en el tratamiento de los datos personales, a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.
- Aplicar las medidas mínimas de protección de datos, establecidas en las presentes políticas.
- Implementar los controles operacionales y las medidas mínimas complementarias necesarias para solventar los riesgos y amenazas de conformidad con el Sistema de Gestión de Seguridad lo establezca.
- Las demás que establezcan la Ley 316 de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Veracruz y el Reglamento Interno de esta Comisión.

## 7. Supresión de Datos

La baja archivística de la documentación o bases de datos que contengan datos personales, deberá realizarse conforme a la normatividad vigente que resulte aplicable en la eliminación, borrado o destrucción de los datos bajo las medidas de seguridad previamente establecidas.

Una vez que los datos han cumplido con las finalidades previstas y cumplido el tiempo de conservación asignado en el sistema de protección, mismo que deberá corresponder con el Catálogo de Disposición Documental de la CEDH, podrá llevarse a cabo su supresión.

El procedimiento de baja de los datos personales atenderá a los procesos establecidos por la Unidad de Archivos de esta Comisión, de conformidad con la normatividad que resulte aplicable, o en su caso, a petición del Titular, en ejercicio de los derechos ARCO.

## Principios y Deberes que rigen el tratamiento de Datos Personales

### 8. Principios

En todo tratamiento, las y los servidores públicos de la CEDH en su calidad de "responsables" y los particulares en su calidad de "encargados" de los datos personales de la CEDH deberán observar los siguientes principios:

#### 8.1. Licitud

Para el tratamiento de datos personales, los servidores públicos deberán sujetarse a las facultades o atribuciones que el Reglamento Interno les confiere, respetando en todo momento los derechos y libertades de los titulares.

#### 8.2. Finalidad

Todo tratamiento realizado por los servidores públicos de la CEDH deberá estar justificado por finalidades concretas (atienda a fines específicos), lícitas (acorde a sus atribuciones o facultades), explícitas (señaladas de manera clara en el aviso de privacidad) y legítimas (con pleno consentimiento del titular, salvo que exista una causal de excepción de acuerdo con la Ley.)

#### 8.3. Lealtad

El tratamiento de datos personales no deberá realizarse a través de medios engañosos o fraudulentos, entendido a éstos cuando: medie dolo, mala fe o negligencia; se realice un tratamiento que genere una discriminación; o se vulnere la expectativa razonable de protección (engaño) por parte del servidor público.

#### 8.4. Consentimiento

Los servidores públicos de la CEDH que recaben datos personales están obligados a obtener el consentimiento del titular, salvo que se actualice una de las causales establecidas en el artículo 16 de la Ley.

El consentimiento del titular deberá otorgarse de manera:

- Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
- Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e
- Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

El consentimiento podrá expresarse de manera expresa o tácita. Por regla general, será válido el consentimiento tácito que se obtiene al informar o poner a la vista de la persona Titular el aviso de privacidad, salvo que la Ley exija que sea expreso.

Cuando los datos sean recabados indirectamente de la persona Titular, no podrán ser tratados hasta en tanto se cuente con la manifestación de la voluntad libre, específica e informada de la misma, salvo que se actualice una causal de excepción de las mencionadas en la Ley.

Cuando se traten datos sensibles, se deberá obtener el consentimiento expreso y por escrito de la persona Titular, para lo cual se deberá facilitar un medio sencillo y gratuito para la manifestación de la voluntad en la cual se plasme la firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable.

Para el tratamiento de datos personales de Niñas, Niños y Adolescentes deberá sujetarse a las reglas de representación previstas en la Legislación Civil del estado y atendiendo siempre al principio de interés superior de la niñez.

### 8.5. Calidad

Los datos personales recabados por los Servidores públicos de la CEDH en cumplimiento de sus funciones deberán ser: exactos, completos, correctos y actualizados a fin de garantizar la veracidad de éstos. Se presume la veracidad de los mismos, cuando son proporcionados directamente por su titular.

### 8.6. Proporcionalidad

Sólo se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento; es decir, sólo se deberán tratar los datos mínimos necesarios para prestar el servicio requerido por el titular.

### 8.7. Información

Los servidores públicos que recaben datos personales, deberán informar al Titular sobre la existencia del Aviso de Privacidad y el tratamiento al que serán sometidos sus datos personales.

### 8.8. Responsabilidad

Las áreas responsables del tratamiento de datos personales deberán implementar los mecanismos necesarios para asegurar el cumplimiento de los deberes, principios y obligaciones que establece la Ley.

### 9. Deberes

En todo tratamiento de datos personales, los servidores públicos de la Comisión tendrán la obligación de respetar los deberes de seguridad y confidencialidad de la información.

**9.1 Seguridad.-** Se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

**9.2 Confidencialidad.-** Se refiere a guardar secreto o sigilo sobre los datos personales objeto de tratamiento, tampoco deberán divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley.

## De los tipos, medidas y niveles de seguridad

### 10. Tipos de seguridad

De conformidad con la Ley 316, las áreas responsables de Sistemas de Protección de Datos Personales podrán establecer (atendiendo a la naturaleza de la información) los siguientes tipos de seguridad:

**10.1 Física:** A la medida orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

**10.2 Lógica**: A las medidas de seguridad administrativas y de protección que permiten la identificación y autenticación de las usuarias y los usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

**10.3 De desarrollo y aplicaciones**: A las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las usuarias y usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas.

10.4 De cifrado: A la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información.

10.5 De comunicaciones y redes: A las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

10.6 Básicas: Son medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales como el registros de funciones y obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales; registro de vulneraciones; identificación y autenticación; control de acceso; gestión de soportes; y copias de respaldo y recuperación.

## 11. Medidas de seguridad

Los datos personales, sólo puede ser recopilados y tratados por las áreas establecidas en el aviso de privacidad y su correspondiente sistema de protección; es decir, aquellas que cuentan con atribuciones para hacerlo.

Toda transferencia de datos personales deberá estar fundada, motivada y acorde al Sistema de Protección correspondiente. Las y los servidores públicos al realizar una transferencia de datos deberán hacer del conocimiento de su receptor la obligación de resguardar los datos de conformidad con el aviso de privacidad con el cual fueron recabados y las finalidades que éste persigue.

Las medidas de seguridad a las que se refiere este apartado constituyen los mínimos exigibles, por lo que cada área de esta Comisión podrá adoptar las medidas adicionales que estime necesarias para el tratamiento de los datos personales que lleve a cabo. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales.

11.1 Seguridad física y ambiental. Se refiere al establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo, con el fin de prevenir:

- Accesos no autorizados.
- Daño parcial a documentos por malas prácticas o falta de espacios adecuados para su resguardo de las condiciones ambientales.
- Robo o pérdida de documentos físicos, entre otros.

11.2 Seguridad Técnica: Son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

- Gestión de comunicaciones y operaciones. (Medidas de protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento, etc.).

- Control de acceso. (Medidas de gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información).

- Adquisición, desarrollo, uso y mantenimiento de sistemas de información. (Procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros).

11.3 Seguridad Administrativa: Son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

- Política de seguridad. (Directrices estratégicas en materia de seguridad de activos).
- Cumplimiento de la normatividad. (Establecimiento de controles para evitar violaciones de la normatividad vigente).
- Organización de la seguridad de la información. (Establecimiento de controles y designación de responsables, que garanticen la seguridad de la información).
- Clasificación y control de activos. (Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable).
- Seguridad relacionada a los recursos humanos. (Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral).
- Administración de incidentes (vulneraciones). (Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información).
- Continuidad de las operaciones. (Medidas para contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas por una vulneración de la información. Ej. Pérdida de información necesaria para la continuidad de un expediente.)

## 12. Niveles de Seguridad

En función del tipo de información tratada, las áreas responsables deberán implementar los siguientes niveles de seguridad:

12.1 Básico: Son las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos que contengan datos personales.

12.2 Medio: Medidas de seguridad que se deben adoptar cuando se tratan bases de datos relacionadas con sistemas o expedientes relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como las que contengan información suficiente que permita obtener una evaluación de la personalidad de un individuo.

12.3 Alto: Medidas de seguridad que se deben aplicar a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos.

Los responsables deberán incluir la aplicación de los Controles Sugeridos como gestión de riesgos para prevenir, identificar y analizar los posibles riesgos y amenazas, así como sus causas o consecuencias de conformidad con el Sistema de Gestión de Seguridad. Dichos controles son aplicables en cualquier tratamiento de datos personales.

## Implementación del Plan de Respuesta a Vulneraciones

### 13. Accidentes, siniestros o vulneraciones

Ante la detección de una posible vulneración, la o el servidor público que la haya detectado deberá dar aviso inmediato al Titular del área responsable del Sistema de Protección, para que éste de inicio al plan de respuesta a vulneraciones, concretando acciones específicas que permitan resolver la brecha, minimizar sus consecuencias y evitar que vuelva a suceder en el futuro.

De conformidad con la Ley, se consideran vulneraciones:

1. La pérdida o destrucción no autorizada.
2. El robo, extravío o copia no autorizada.
3. El uso, acceso o tratamiento no autorizado, o
4. El daño, alteración o modificación no autorizada.

El Titular del área responsable del Sistema deberá informar dentro de las primeras 72 horas en que tuvo conocimiento del incidente sobre la vulneración detectada. Para tales efectos, se consideran áreas competentes dentro de la CEDH, las siguientes:

Unidad de Transparencia. Para efectos de brindar asesoría y acompañamiento en la implementación del plan de respuesta, y en su caso informar al Órgano garante.

Órgano de Control Interno. Para efectos de investigar y determinar posibles responsabilidades de las y los servidores públicos de acuerdo a su competencia.

El área responsable deberá rendir un informe final cuando haya concluido las etapas del plan de respuesta. Durante el proceso, deberá recabar evidencias respecto de lo ocurrido y las acciones tomadas para efectos de elaborar el informe correspondiente.

El plan de respuesta a vulneraciones se conformará de las siguientes etapas:

1. Identificación;
2. Contención;
3. Erradicación;
4. Recuperación; e
5. Informe.

### 13.1 Identificación:

Consiste en la revisión que deberá realizar el área responsable a fin de identificar si existen indicadores que demuestren que los activos han sido afectados. Por sí mismo un solo evento o alerta de seguridad, no implica necesariamente la materialización de un incidente.

### 13.2 Contención:

La o el titular deberá tomar las decisiones inmediatas que de acuerdo con el tipo de información comprometida permitan detener momentánea o definitivamente la vulneración detectada.

### 13.3 Erradicación

En el proceso de erradicación el área responsable del Sistema de Protección deberá identificar y de ser posible solventar los efectos de la vulneración.

Con objeto de planificar la respuesta al incidente se deberá fijar un plazo razonable para la implementación de esta etapa.

### 13.4 Recuperación

Una vez que la vulneración ha sido solucionada y solventado sus efectos, se dará inicio a la etapa de recuperación; la cual tiene como objetivo, el restablecimiento de la operatividad del sistema, base o expediente involucrado. Puede implicar la adopción no solo de medidas activas, sino de controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

### 13.5 Informe

Una vez concluidas las etapas de contención, erradicación y recuperación, el área responsable del Sistema de Protección elaborará un informe que presentará a la Contraloría Interna y Unidad de Transparencia, que deberá contener:

1. Descripción objetiva del incidente, que contenga:

- Medio por el que se ha materializado la brecha o tipo de vulneración; es decir, qué ha ocurrido: se ha perdido un dispositivo con datos personales, se ha producido un robo de equipos, dispositivos o documentos que contengan datos personales, se han publicado datos personales por error o se ha enviado a un destinatario equivocado, un ransomware (secuestro de datos) ha cifrado un dispositivo, se ha producido una intrusión no autorizada en un sistema de información con datos personales, un servidor público ha sido víctima de phishing (suplantación de identidad), etc.
- Origen de la brecha (vulneración), si ha sido interna o externa y su intencionalidad.
- Categorías de datos: si son datos básicos identificativos o de contacto o si bien, son categorías especiales como pueden ser datos sensibles, sobre la salud, de las víctimas de violaciones, situación patrimonial de los servidores públicos, etc.
- Volumen de datos afectados, tanto en número de registros afectados como en número de personas afectadas.
- Categorías de afectados: quejosos, servidores públicos, prestadores de servicio social (estudiantes), proveedores o víctimas de violaciones graves de derechos humanos, etc.
- Información temporal de la brecha (vulneración): cuándo se inició, cuándo se ha detectado y cuándo se resolvió o resolverá la brecha de seguridad.
- Controles existentes en el momento del incidente.

2. Enumeración de medidas efectivas de respuesta.

3. Medidas de contención, erradicación y recuperación aplicadas.

4. Informe a interesados: Los responsables deberán informar a la persona o personas Titulares y al Instituto las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que las o los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Para lo anterior, se procederá en términos de los artículos 41 fracción XII y 54 de la Ley.

## Responsabilidades y sanciones

### 14. Responsabilidades

Incurrir en actos u omisiones que incumplan o transgredan las obligaciones conferidas por el Reglamento Interno de esta Comisión estatal y la Ley 316 en materia de Protección de Datos Personales generará una responsabilidad por parte de las servidoras o servidores públicos.

Los incumplimientos a las obligaciones establecidas por la Ley 316 y las establecidas en las presentes Políticas Internas detectados por la Unidad de Transparencia, serán informados al Órgano Interno de Control de esta Comisión Estatal de Derechos Humanos, a fin de que en el ejercicio de sus atribuciones determine la posible responsabilidad en que incurran las y los servidores públicos.

Adicional a lo anterior, en caso de que el Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales (IVAI) notifique a la Unidad de Transparencia un presunto incumplimiento deberá observarse lo dispuesto por la Ley 316.

Serán causas de sanción por incumplimiento:

- Incumplir los plazos de atención previstos en la Ley para responder solicitudes de derechos ARCO.
- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- Dar tratamiento a los datos personales en contravención a los principios y deberes establecidos en la Ley;
- No contar con el aviso de privacidad;
- Omitir en el aviso de privacidad alguno de los elementos a que refieren los artículos 30, 31 y 32 de la Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
- Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
- Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley;
- No establecer las medidas de seguridad en los términos que establecen los artículos 42, 43, 44 y 45 de la Ley;
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 42, 43, 44 y 45 de la Ley;
- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley;
- Obstruir los actos de verificación;
- Crear bases de datos personales en contravención a lo dispuesto en la Ley;

- Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;
- Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos y en la Constitución Política del Estado; y
- Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO.

Adicional a lo anterior, se considerará como incumplimiento la falta de aplicación de las presentes Políticas en el tratamiento de los datos personales de acuerdo con el artículo 201 fracciones III y VI del Reglamento Interno de esta Comisión.

### 15. Sanciones

Para tales efectos, en caso de que el incumplimiento sea comprobado por el Instituto, éste podrá imponer las medidas de apremio señaladas en la Ley 316 para asegurar el cumplimiento de sus determinaciones.

En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 179 de la Ley, se deberán denunciar los hechos ante la autoridad competente.

Las medidas de apremio de carácter económico impuestas por el Instituto no podrán ser cubiertas con recursos públicos. De acreditarse un incumplimiento, de conformidad con el artículo 169 de la Ley, la o el servidor público responsable podrá ser acreedor a:

- Amonestación pública o;
- Multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la unidad de medida y actualización. En caso de reincidencia podrá ampliarse al doble.

Sin perjuicio de lo anterior, la Contraloría Interna podrá iniciar los procedimientos que considere necesarios para investigar y sancionar los incumplimientos a las presentes Políticas en términos del Reglamento Interno de esta Comisión.

## Mecanismo de monitoreo y control

### 16. Monitoreo

El funcionamiento de las políticas internas y medidas preventivas será monitoreado a través de los procedimientos de mejora continua que se realicen para la actualización bianual del Sistema

de Gestión, en el que participarán todas las áreas administrativas de la Comisión Estatal involucradas en el tratamiento de datos personales y en los demás casos establecidos en el artículo 49 de la Ley.

La Etapa de monitoreo podrá incluir solicitudes de informes y revisiones a las áreas para dar seguimiento al cumplimiento del Sistema.

### 17. Evaluación

La evaluación de las medidas implementadas se realizará a través de procedimientos de revisiones periódicas anuales o semestrales realizadas por la Unidad de Transparencia. Adicionalmente, podrán llevarse a cabo auditorías para verificar el cumplimiento del Sistema, por parte de la Unidad de Transparencia y la Contraloría Interna en términos de los artículos 52 fracción III y 90 fracción XVII del Reglamento Interno de esta Comisión.

Para el desarrollo de auditorías, se utilizarán los formatos y procedimientos sugeridos por el Órgano Interno de Control de este Organismo.

## II. MEDIDAS DE SEGURIDAD APLICABLES POR NIVEL DE PROTECCIÓN

El artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz, establece que los responsables deberán adoptar las medidas de seguridad considerando los tipos de seguridad y niveles de seguridad establecidos conforme a las características propias de la información. Por lo anterior, en cumplimiento a dicha disposición, la implementación de medidas de seguridad atenderá al nivel de protección que cada sistema de datos del Organismo tiene establecido.

A continuación, se presenta la clasificación de Sistemas de Datos de Acuerdo al Nivel de Protección:

| Nivel de Seguridad | Sistemas de Datos Personales | Políticas Internas Aplicables | Tipos de Medidas aplicables |
|---|---|---|---|
| Básico | • Sistema de Datos Personales del Control de Registro de Acceso a las Instalaciones de la CEDH Veracruz.<br>• Sistema de Datos de las Organizaciones de la Sociedad Civil. | Medidas Mínimas Físicas, Técnicas y Administrativas | A a la G |

| | | | |
|---|---|---|---|
| | • Sistema de Datos Personales de los Expedientes de Solicitudes de Acceso a la Información y Derechos ARCO de la CEDH Veracruz.<br>• Sistema de Datos Personales del Registro de Participantes a Cursos, Talleres, Diplomados u otras Actividades de Capacitación, Organizadas en Colaboración con otras Instituciones de la CEDH Veracruz.<br>• Sistema de Datos Personales de Registro de Periodistas y Medios de Comunicación de la CEDH Veracruz.<br>• Sistema de Datos Personales de las Redes Sociales de la CEDH Veracruz.<br>• Sistema de Datos Personales de la Recopilación de Evidencias de las Actividades de la CEDH Veracruz.<br>• Sistema de Datos Personales del Registro de Asistencia a Eventos de la Unidad de Atención a Niñas, Niños y Adolescentes.<br>• Sistema de Datos Personales del Registro de Asistentes a Reuniones de Trabajo y Vinculación de la Secretaría Ejecutiva de la CEDH Veracruz.<br>• Primer Concurso de Dibujo elaborado por niñas, niños y adolescentes, organizado por la CEDHV.<br>• Convocatoria para Ocupar Vacantes Ciudadanas del Consejo Consultivo de Gobierno Abierto de la CEDHV. | | |
| Medio | • Sistema de Datos Personales de los Recursos Humanos.<br>• Sistema de Datos Personales de los Expedientes de los Prestadores del Servicio Social.<br>• Sistema de Datos Personales de los Expedientes sobre las Declaraciones Patrimoniales y de Intereses de los Servidores Públicos de la Comisión Estatal de Derechos Humanos de Veracruz.<br>• Sistema de Datos Personales del Padrón de Proveedores de la Comisión Estatal de Derechos Humanos Veracruz.<br>• Sistema de Datos Personales de Resolución del Recurso de Revocación de la Comisión Estatal de Derechos Humanos de Veracruz.<br>• Sistema de Datos Personales de Responsabilidades, Faltas Administrativas, Quejas y Sanciones de los Servidores Públicos de la Comisión Estatal de Derechos Humanos de Veracruz.<br>• Sistema de Datos Personales de Denuncias ante la Fiscalía Especializada en Combate a la Corrupción de la Comisión Estatal de Derechos Humanos de Veracruz. | Medidas Mínimas Físicas, Técnicas y Administrativas | A a la K |

| | | | |
|---|---|---|---|
| | • Sistema de Datos Personales de las Actividades de la Unidad para la Igualdad de Género.<br>• Sistema de Datos Personales del Monitoreo de Albergues para Migrantes.<br>• Sistema de Datos Personales de las Actas Administrativas y de Entrega-Recepción de los Servidores Públicos de la Comisión Estatal de Derechos Humanos de Veracruz. | | |
| Alto | • Sistema de Datos Personales de solicitudes de intervención, quejas, recursos y seguimiento de resoluciones<br>• Sistema de Datos Personales de Asistencia a Víctimas para su Incorporación al Registro Estatal de Víctimas por parte de la CEDH Veracruz.<br>• Sistema de Datos Personales de Entrevistas para la Emisión de Dictámenes de Valoración de Impacto y aplicación de Protocolos de Estambul de la CEDHV.<br>• Sistema de Datos Personales del Registro de Participantes en Eventos del Consejo Consultivo, y Actividades de Difusión y Capacitación de la CEDHV | Medidas Mínimas Físicas, Técnicas y Administrativas | A a la N) |

Atendiendo a la anterior clasificación, los responsables de los Sistemas de Datos deberán implementar las medidas de seguridad de conformidad con los tipos, niveles y categorías (ver apartado de normatividad) que correspondan al nivel de protección y de conformidad con los controles establecidos en el Sistema de Gestión, con base en lo siguiente:

## Medidas por Nivel de Seguridad

### a) Documento de seguridad

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

Por lo anterior, todos los sistemas con independencia del nivel de seguridad, deberán constar en el documento de seguridad de la CEDH y apegarse a las políticas establecidas con motivo del mismo.

### b) Funciones y Obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales

Descripción: Aspecto que contempla la descripción de las funciones y obligaciones que de acuerdo con la normatividad aplicable a la Comisión Estatal de Derechos Humanos y los manuales de procedimientos, los servidores públicos deben cumplir.

La relación de funciones y obligaciones que consta en el documento de seguridad, será la guía para la asignación de privilegios al personal, en el tratamiento de datos personales. Es decir, deberá existir una correspondencia entre el puesto que desempeñe el servidor, las funciones asignadas y los accesos para el tratamiento de datos personales.

### c) Registro de vulneraciones

Cualquier suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales, se considerará una vulneración en términos de la normatividad aplicable y tendrá como consecuencia inmediata la activación del Plan de Respuesta a Vulneraciones establecido en las Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de Datos Personales en Posesión de la CEDHV.

Las áreas administrativas deberán llevar un registro de las vulneraciones detectadas en una bitácora de registro de vulneraciones que contendrá lo siguiente:

Bitácora de registro de vulneraciones (Anexo I.1)

Lo anterior, no exime al responsable de implementar todas las etapas del plan de respuesta establecido en las Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de los Datos Personales en la CEDHV y del llenado del "Formato de Bitácora de Vulneraciones" que le corresponde. (Anexo I.2)

### d) Identificación y Autenticación

Descripción: La autenticación es el proceso de identificación del servidor público a partir de contraseñas, credenciales o algún otro procedimiento.

Así, al establecer mecanismos de acceso a los usuarios podemos asegurar la integridad, confidencialidad y disponibilidad de la información al garantizar que sólo las personas autorizadas accedan a dichos activos, documentar estos procedimientos y en general controlar los accesos.

El objetivo de este procedimiento es garantizar el acceso seguro a los sistemas de datos autentificando la identidad de los usuarios.

Para la implementación de medidas de seguridad en etapas en el control de acceso, las áreas administrativas deberán considerar lo siguiente:

I. **Identificar:** Deberán implementar acciones para verificar que una persona es quien dice ser, acredita su personalidad exhibiendo una identificación oficial, o en un ambiente electrónico,

ingresa con el nombre de usuario y contraseña establecida para el desarrollo de sus funciones. (*login/password*).

II. **Autenticar:** En su caso, deberán implementar acciones que permitan comprobar que esa persona es quien dice ser a través del cotejo de uno o más datos contenidos en una identificación oficial, firmas, contraseñas, números de expedientes o cualquier otra información oficial que la persona deba conocer.

III. **Autorizar:** Se refiere al permiso a la persona que se ha identificado y autenticado apropiadamente y depende del o de los permisos que le conceda el responsable de otorgar los accesos.

- Procedimiento de identificación y autenticación de acceso a los sistemas de datos. El responsable del sistema deberá asegurarse de llevar a cabo al menos las siguientes actividades:

1. Contar con una relación actualizada de servidores públicos que tengan acceso autorizado al sistema de datos (altas y bajas de usuarios). Dicha relación deberá ser coincidente con las funciones y obligaciones del personal establecidas en la normatividad interna, ya sea Ley, Reglamento Interno o en los manuales de procedimientos del área.
2. Recursos asignados (control de dispositivos de almacenamiento institucionales que contienen datos).
3. Para el acceso a bases de datos internas de sistemas de datos. Se deberá establecer un proceso de generación y/o asignación de contraseñas. Se sugiere establecer su longitud: mínimo 8 caracteres; uso de letras: entre mayúsculas y minúsculas; números y signos. Asimismo, establecer la actualización periódica de acuerdo a las necesidades del área y el nivel de protección del sistema que le corresponda.
4. La asignación de contraseñas para el acceso a bases de datos internas, podrá realizarse directamente por el responsable del sistema, en cuyo caso deberá mantener una relación actualizada de las contraseñas asignadas y de los permisos sobre los recursos asignados: (lectura, escritura, modificación*)*.
5. La identificación y autenticación para el acceso a sistemas "generales" de la CEDH Veracruz, correrá a cargo de la Dirección de Informática y Estadística.
   (Anexo II)

### e) Control de acceso

Descripción: Estrechamente relacionado con el procedimiento de identificación y autenticación, tenemos el control de acceso. Este proceso, implica que el responsable del sistema de datos personales deberá adoptar medidas para que los encargados del tratamiento de datos personales y

usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Por ello, es fundamental la implementación y correcto llenado de las bitácoras de accesos, así como el mantener una relación actualizada del personal, el tipo de funciones que desempeñan y los accesos que de acuerdo con sus atribuciones tienen autorizadas.

Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el sistema de datos personales. Solamente el responsable del sistema de datos personales podrá conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.

- Proceso de control de acceso. Para llevar a cabo un correcto proceso de control de acceso, los responsables de los sistemas deberán llevar a cabo lo siguiente:

1. Contar con una relación actualizada del personal, sus facultades de acuerdo con el Reglamento Interno o manuales del área y el tipo de información al que tiene acceso autorizado.
2. En concordancia con el procedimiento de identificación y autenticación: Establecer una bitácora de registro de accesos a los expedientes o información que conforman los sistemas de datos, en la que se registrarán todos los accesos tanto del personal autorizado, como en su caso de consultas extraordinarias (quejosos, abogados externos, otras áreas involucradas) a fin de poder determinar accesos no autorizados y las responsabilidades en caso de una vulneración.
3. Para el acceso de personal externo a los expedientes que conforman el sistema, el responsable deberá además verificar que la persona solicitante cumplió con todos los filtros del control de acceso a las instalaciones de la CEDHV; es decir, que fue registrado debidamente, que cuenta con un gafete de autorización a su área y solicitar una identificación en la que conste ser la persona que refiere ser. Lo anterior, a fin de evitar vulneraciones a la seguridad de los datos. Anexo III

### f) Gestión de soportes

Descripción: Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal se deberá cuidar que estén etiquetados para permitir identificar el tipo de información que contienen, ser inventariados y sólo podrán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, fuera de las instalaciones u oficinas bajo el control del responsable del sistema de datos personales, deberá ser autorizada por éste, o encontrarse debidamente autorizada en el documento de seguridad. En el traslado de soportes físicos y electrónicos se adoptarán medidas dirigidas a evitar la sustracción,

pérdida o acceso indebido a la información durante su transporte. Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

### g) Copias de respaldo y recuperación

Descripción: La realización de copias de respaldo de los sistemas o bases que contengan datos personales que obren en la "nube" de la CEDHV estará a cargo de la Dirección de Informática y Estadística, quien establecerá la periodicidad de su realización conforme a las necesidades específicas de cada sistema de información o base de datos.

Para lo anterior, el responsable de la realización de las copias, deberá llevar una bitácora de respaldos, con la finalidad de detectar cualquier vulneración, en la que establecerá la periodicidad y los datos que permitan determinar en su momento la responsabilidad en relación a la elaboración de las copias de respaldo con base en el formato sugerido. Anexo IV

Adicional a lo anterior, el área administrativa responsable del sistema de datos podrá (deberá) realizar verificaciones periódicas de las copias de respaldo y recuperación realizadas por la Dirección de Informática y Estadística. Para ello, el responsable deberá establecer la periodicidad con que se realizarán y seguir las recomendaciones establecidas en el apartado "pruebas con datos reales".

Los resultados negativos de estas pruebas deberán documentarse con la finalidad de que se puedan establecer o mejorar los controles que permitan subsanar la brecha localizada.

### h) Responsable de seguridad

Descripción: El responsable del sistema de datos personales designará uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación no implica una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales de acuerdo con la Ley y los Lineamientos (Titular del área). Se refiere a aquella persona designada por el responsable del sistema de datos para dar seguimiento y controlar la correcta aplicación de las medidas de seguridad físicas, técnicas y administrativas establecidas para garantizar la confidencialidad y seguridad de los datos personales.

Figura del responsable de medidas de seguridad

De conformidad con el artículo 43 apartado B fracción II inciso a), dentro del nivel medio de seguridad, el responsable del sistema de datos de forma adicional a las medidas de seguridad básicas, considerará la designación de un responsable de seguridad.

El responsable de seguridad designado por el titular del área como responsable del sistema de datos, dará seguimiento a la correcta implementación de las medidas de seguridad y fungirá como coordinador de las mismas al interior del área administrativa. Dicho lo anterior, cada área

administrativa responsable de un sistema de datos, deberá designar a un responsable de seguridad, para lo cual deberá tomar en cuenta lo siguiente:

A fin de facilitar sus funciones y llevar a cabo un correcto seguimiento, la persona dedignada deberá cumplir los siguientes requisitos:

1. Ser parte del área responsable del sistema y tener pleno conocimiento de las atribuciones del área.
2. Deberá conocer las obligaciones que en materia de protección de datos personales adquieren los servidores públicos.
3. Tener conocimiento del sistema de datos que corresponde al área, así como de las medidas físicas, técnicas o administrativas mínimas implementadas para la seguridad de los datos.

El responsable de seguridad tendrá entre sus funciones las siguientes:

1. Vigilar la implementación en tiempo y forma de las medidas de seguridad que sean aplicables al sistema que le corresponda.
2. Coordinar en el área la implementación de las medidas físicas, técnicas y administrativas mínimas exigibles.
3. Reportar al responsable del sistema cualquier incumplimiento en las medidas o vulneración de datos que sea detectada dentro de su área o inclusive en cualquier otra que tenga impacto en la seguridad de los datos de la CEDHV.
4. Implementar junto con el responsable(s) del sistema las medidas de seguridad adicionales que consideren convenientes para garantizar la integridad, disponibilidad y seguridad de la información.
5. Rendir los informes de avances ante el responsable del sistema de datos para efectos de solventar los requerimientos realizados por la Unidad de Transparencia y/o la Contraloría Interna.

## Anexo V

### i) Auditoría

Descripción: Proceso implementado como parte de la etapa de seguimiento y evaluación al Sistema de Gestión, en el que se pretende llevar a cabo una revisión de los controles establecidos, auditar los accesos a los datos y conocimiento de las políticas internas con la finalidad de evaluar y/o detectar riesgos potenciales de vulneraciones.

Para su implementación se seguirán el siguiente procedimiento:

1. Planeación;

2. Cronograma de actividades;

3. Orden de Auditoría;

4. Procedimiento de auditoria;

5. Seguimiento

## Anexos VI

### j) Control de acceso físico

Descripción: El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o electrónico, deberá permitirse exclusivamente a quienes estén expresamente autorizados en el documento de seguridad.

Para permitir el acceso físico al sistema de datos el responsable deberá asegurarse que se agotaron todos los filtros establecidos para garantizar la seguridad y confidencialidad de la información, para lo cual se seguirán las siguientes recomendaciones:

Medidas de control para usuarios del sistema:

- Acceder a los equipos utilizando claves de usuario y contraseñas
- La autoidentificación para los equipos de cómputo y bases, debe hacerse a través de canales cifrados y haciendo uso de contraseñadas renovadas periódicamente.
- Realizar los accesos sólo a través de equipos institucionales y dentro de las oficinas, salvo autorización expresa de su titular.
- El acceso a expedientes (documentos físicos) deberá registrarse en la bitácora del área.
- Para el acceso a equipos de cómputo y expedientes físicos, el servidor público deberá contar con facultades establecidas en la normatividad interna.

Medidas de control para particulares

- Identificarse para el acceso a las instalaciones de la CEDHV como primer filtro.
- Contar con un gafete de acceso permitido al piso o área en el que se encuentra.
- Identificarse como titular de los datos ente el personal del área al que acude a realizar una consulta.
- En caso de que el acceso se solicite vía telefónica, el titular deberá acreditar su identidad proporcionando los datos requeridos por el responsable para asegurarse de que éste es quien dice ser y evitar vulnerabilidades por fuga de información.
- En ningún caso, se permitirá a los particulares la consulta directa al sistema o base de datos que contiene su información, ya que éstos contienen datos de más titulares y por tanto no es una fuente de acceso público.
- La autoidentificación para los equipos de cómputo y bases, debe hacerse a través de canales cifrados y haciendo uso de contraseñadas renovadas periódicamente.

## k) Pruebas con datos reales

Descripción: Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados.

Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo que garantice la integridad de la información que formará parte de la prueba.

Anualmente como parte del proceso de mejora continua del Sistema de Gestión, la Unidad de Transparencia realizará la prueba con datos reales con la información respaldada por la Dirección de Informática y Estadística a fin de monitorear la eficiencia y seguridad de las pruebas de respaldo y recuperación.

Adicionalmente, las áreas administrativas responsables de los Sistemas de Datos con nivel medio y alto, deberán monitorear la disponibilidad e integridad de su información respaldada por parte de la Dirección de Informática de forma periódica (semestral, o trimestral o según la relevancia de su información) y asentar evidencia de los resultados obtenidos en caso de que la prueba tenga como resultado la detección de una alerta de seguridad (es decir, que la información se encuentre comprometida).

## l) Distribución de soportes

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión.

Los responsables de las áreas administrativas deberán mantener un control de los soportes automatizados (dispositivos electrónicos institucionales) con los cuales se comprarte, trasfiere o traslada información, desde su asignación hasta su eventual devolución o destrucción.

## m) Registro de acceso

El acceso a los sistemas de datos personales se limitará exclusivamente al personal autorizado, estableciendo mecanismos que permitan identificar los accesos realizados en el caso de que los sistemas puedan ser utilizados por múltiples autorizados.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad correspondiente, sin que se permita la desactivación o manipulación de los mismos. De cada acceso se guardarán:

- Identificación del usuario
- Fecha y hora en que se realizó
- Sistema accedido
- Tipo de acceso y si éste fue autorizado o denegado

El periodo de conservación de los datos consignados en el registro de acceso será de al menos 2 años.

### n) Telecomunicaciones

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

En todo caso, se deberán identificar las barreras de seguridad y controles de entrada con que cuenta cada área, tales como: escaleras, muros, puertas de salida de emergencia, puertas con control de acceso a través de llave o cualquier otro medio que el avance de la tecnología permita, a fin de evitar accesos no autorizados al perímetro de los archivos institucionales o de las bases de datos.

## Anexos

Anexo I. 1 **Formato de Registro de Vulneraciones**

| Fecha en que ocurrió | Tipo de Vulneración | Fecha de la Bitácora | Fecha en que se resolvió |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Anexo I.2 **Formato Bitácora de Vulneraciones**

| BITÁCORA DE VULNERACIONES | | |
|---|---|---|
| (Complete el contenido del siguiente formulario en caso de detectar cualquier vulneración) | | |
| FECHA DE INICIO DE LA VULNERACIÓN: | FECHA EN QUE SE DETECTÓ: | FECHA EN QUE SE RESOLVIÓ O RESOLVERÁ: |
| ÁREA | | |
| RESPONSABLE DEL ÁREA | | |
| SISTEMA DE INFORMACIÓN, BASE DE DATOS O EXPEDIENTE VULNERADO | | |
| SOPORTE DE LA INFORMACIÓN VULNERADA | Físico ☐ Automatizado ☐ Combinado ☐ | |
| TIPO DE VULNERACIÓN | Pérdida o destrucción no autorizada ☐<br>Robo, extravío o copia no autorizada ☐<br>Uso, acceso o tratamiento no autorizado ☐<br>Daño, alteración o modificación no autorizada ☐ | |
| ORIGEN | Interno ☐ Externo ☐ | |
| CATEGORÍA DE DATOS COMPROMETIDOS | ☐ Identificativos ☐ laborales<br>☐ Académicos ☐ electrónicos<br>☐ De la salud ☐ patrimoniales<br>☐ Sobre procedimientos administrativos<br>☐ De tránsito o movimientos migratorios<br>☐ Sensibles. Especifique: _____ | |
| VOLUMEN Y CATEGORÍA DE AFECTADOS | Número de afectados: _____<br>Categoría (servidores públicos, víctimas, quejosos, etc.):<br>_____ | |

<table>
<tr><td>CONTROLES EXISTENTES AL MOMENTO DEL INCIDENTE</td><td colspan="2">Enuncie las medidas con las que contaba el área para la protección del sistema de información:</td></tr>
<tr><td>MEDIDAS DE RESPUESTA APLICADAS</td><td colspan="2"><table><tr><th>Contención</th><th>Erradicación</th><th>Recuperación</th></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>_____<br>NOMBRE Y FIRMA DE QUIEN REPORTA</td><td>_____<br>NOMBRE Y FIRMA DE QUIEN ADMINISTRA EL SISTEMA</td><td>_____<br>NOMBRE Y FIRMA DEL TITULAR DEL ÁREA</td></tr>
</table>

Anexo II. **Formato registro de Identificación y Autenticación**

| Servidor | Funciones y Obligaciones (Fundamento) | Recursos Asignados | Bases o Sistemas a los que tiene acceso | Tipo de privilegio | Contraseña asignada | Última modificación |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Anexo III. **Formato Control de Acceso**

| BITÁCORA DE ACCESO | | | | |
|---|---|---|---|---|
| (Deberá registrarse cualquier acceso del personal del área que no tiene bajo su resguardo dicha documentación o de cualquier otra área que se involucre en la atención) | | | | |
| **Fecha** | **Expediente o documentación consultada** | **Persona que recibe** | **Autorización** | **Observaciones** |
| (fecha en que se realiza la consulta o préstamo) | (número de expediente, oficio, documento o archivo) | (Nombre y firma del servidor a quien se le da acceso) | (nombre y firma del servidor que autoriza) | (registrar cualquier anomalía o vulneración detectada) |
| | | | | |
| | | | | |
| | | | | |

Anexo IV. **Formato Bitácora de Realización de copias de respaldo**

(Periodicidad establecida: _____)

| 1. Fecha de inicio del periodo | 2. Fecha de término del periodo | 3. Servidor público que la realiza | 4. Fecha de realización | 5. Observaciones | 6. Rúbrica |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

Guía de llenado de la hoja de bitácora de respaldo

1. Corresponde indicar el día en que inicia el periodo que corresponde respaldar. Ej. Si el respaldo se realiza semanalmente: Inicio del periodo del __(lunes)/0_/2020
2. Indicar el día en que termina el periodo que corresponde respaldar. Ej. (domingo)/0_/2020
3. Indicar el nombre del servidor público que realiza el respaldo. Ej. Juan Pérez
4. Registrar la fecha en que se lleva a cabo el respaldo. Ej. (viernes)/0_/2020
5. Registrar la duración en horas y minutos que tardó en realizarse la copia de respaldo, y asentar la hora exacta en que se inició y culminó.
6. Registrar cualquier anotación importante observada durante el procedimiento de respaldo: dificultades, pausas, fallas de energía, etc. que puedan servir de referencia al operador o responsable de la base.
7. Asentar la rúbrica del servidor que llevó a cabo el respaldo.

Anexo V. **Formato para la designación de responsable de seguridad (modelo)**

SERVIDOR PÚBLICO_____
PRESENTE

Por este conducto me refiero a las obligaciones que nos impone la Ley de Protección de Datos Personales en posesión de Sujetos Obligados para el estado de Veracruz de Ignacio de la Llave, artículo 43 apartado B, fracción II, inciso a) referente a la designación de los servidores públicos como responsables de seguridad.
En cumplimiento a lo anterior, hago de su conocimiento que en mi calidad de responsable del Sistema de datos -_____, se le designa como Responsable de Seguridad de dicho sistema a cargo de __(área)_____ de la que usted forma parte, para la implementación de las acciones que corresponden al Sistema de Gestión de Seguridad correspondiente.
Para el cumplimiento de su encargo, deberá colaborar en la coordinación de las actividades establecidas en el Documento de Seguridad de la CEDH Veracruz al interior de su área, conforme al nivel de protección del(os) Sistema(s) de Datos del área.
(saludo)…
Atentamente
Nombre, firma y cargo del titular _____
Nombre, firma y cargo del responsable designado. _____
Con copias de conocimiento y efectos

Anexos VI **Formatos del Proceso de Auditoría**

VI.1 **Planeación**

| | | | |
|---|---|---|---|
| Sujeto Obligado: (1) | | | |
| N° de auditoría: (2) | | | |
| Unidad administrativa a auditar: (3) | | | |
| Fecha: (4) | | | |
| Tipo de auditoría: (5) | | | |
| Antecedentes: (6) | | | |
| Objetivo: (7) | | | |
| Alcance (8) | | | |
| Problemática: (9) | | | |
| Estrategia: (10) | | | |
| Personal comisionado: (11) | | | |
| Nombre | Iniciales | Firma | Rúbrica |
| | | | |
| | | | |
| | | | |
| | | | |

| Elaboró (12) | Visto bueno (13) | Autorizó (14) |
|---|---|---|
| (Unidad de Trasparencia) | (Contraloría Interna) | (Contraloría Interna) |
| _____ | _____ | _____ |
| nombre y firma | nombre y firma | nombre y firma |

VI.2. **Cronograma de actividades**

| COMISIÓN ESTATAL DE DERECHOS HUMANOS DEL ESTADO DE VERACRUZ<br>Cronograma de Actividades a Desarrollar | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No. | Actividad | T. Estimado | T. Real | (Calendario de días) | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| _____<br>Elaboró<br>(personal UT) | | | _____<br>Vo.Bo.<br>(Personal C.I.) | | | | _____<br>Autorizó<br>(Personal C.I.) | | | |
| Iniciales<br>T. Estimado: Tiempo estimado para la auditoría<br>T. Real: Tiempo real utilizado. | | | | | | | | | | |

VI. 3. **Orden de Auditoría**

PRESENTE

Con objeto de verificar y promover en esa unidad administrativa el cumplimiento de sus programas sustantivos y de la normatividad aplicable, y con fundamento en lo dispuesto por _____se le notifica que se llevará a cabo en esa dirección/unidad/otro a su cargo, la auditoría número _____ en materia de protección de datos personales.

Para tal efecto se solicita su intervención para que se proporcione a los CC. _____ (documentación a requerir) que soliciten para la ejecución de la auditoría.

Asimismo, comunico a usted que la auditoría se llevará a cabo durante el periodo comprendido del _____ al _____ y estará dirigida a verificar el periodo _____, en la inteligencia de que la auditoria podrá ser ampliada a otros ejercicios de considerarse necesario.

Asimismo, agradeceré girar sus instrucciones a quien corresponda, a fin de que el personal comisionado tenga acceso a los archivos, documentación o información del área a su cargo y se les brinden las facilidades necesarias para la realización de su encargo.

Atentamente

Nombre _____

Cargo _____

VI. 4. Informe de Auditoría y Seguimiento

El informe de auditoría debe incluir los siguientes elementos:

- Título
- Destinatario
- Antecedentes
- Alcance
- Identificación o descripción del Objeto
- Identificación de las Normas de auditoría aplicadas.
- Procedimiento de Auditoría
- Resultados y conclusiones
- Acciones o recomendaciones
- Fecha del Informe
- Firma

Seguimiento

Los auditores deben dar seguimiento a los casos de incumplimiento, cuando proceda.

El formato se registrará conforme a la numeración referida en el mismo, con la información siguiente:

1. Registrar el nombre del sujeto obligado.
2. Anotar el número de auditoria.
3. Anotar el área administrativa que se va a auditar.
4. Indicar el tipo de auditoría que corresponda.
5. Describir el propósito de la revisión.
   Ejemplo: “Verificar la existencia de medidas y controles para garantizar la seguridad de los datos personales”.
6. Describir la documentación requerida para la ejecución del procedimiento, y registrar el fundamento legal que sustente las operaciones objeto de revisión y de la cual se verificará su cumplimiento.
7. Indicar el día, mes y año programados para iniciar y terminar la aplicación del procedimiento de auditoría.
   Ejemplo: dd/mm/aa.
8. Señalar el día, mes y año del inicio y término de la aplicación del procedimiento de auditoría.
   Ejemplo: dd/mm/aa.
9. Marcar con una “x”, en una columna que corresponda, si el procedimiento fue o no aplicado.
10. Anotar los comentarios que el auditor considere importantes, relativos a los hallazgos detectados durante el desarrollo y la aplicación del procedimiento y, en su caso, indicar las causas que motivaron la no aplicación del procedimiento o sus ajustes.
11. Registrar el índice que identifica los papeles de trabajo que le corresponden al procedimiento aplicado y al resultado determinado.
12. Indicar los nombres y cargos de los servidores públicos responsables de la elaboración, revisión y autorización de los procedimientos de auditoría por aplicar.

VI. 5. **Procedimiento de Auditoría**

| | |
|---|---|
| Sujeto Obligado: | Número de auditoría: |
| Área administrativa Auditada: | Sistema de Datos Personales: |
| Tipo de Auditoría:<br>AUDITORÍA INTERNA | Objetivo de la Auditoría:<br>COMPROBAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES |

| N° | Procedimiento | Documentación (requerida para la ejecución del procedimiento) y fundamento legal | Fecha | | | APLICADO | | Comentarios | Ref. Papeles de Trabajo |
|---|---|---|---|---|---|---|---|---|---|
| | | | P/R | Inicio | Término | SI | NO | | |
| | | | | | | | | | |
| 1 | POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES | | | | | | | | |
| | Dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan. | Documentación: | P | | | | | | |
| | | **Fundamento legal:**<br>Artículos 38, fracción V, 43 al 56, 58 y 59 de la Ley PDPPSOEV | R | | | | | | |

**P = Programado**

**R = Real**

| Elaboró | Revisó | Autorizó |
|---|---|---|
| (Personal UTR) | (Personal C.I.) | (Personal C.I.) |
| _____ | _____ | _____ |

## III. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

### Controles derivados de la Matriz de riesgos

A corto, mediano y largo plazo, todas las áreas del Organismo, deberán observar y aplicar los principios, deberes, obligaciones y controles establecidos en las Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de Datos Personales en la CEDH Veracruz.

Los controles a aplicar, contienen medidas de seguridad que podrán identificarse de la siguiente manera:

- Medidas de seguridad física (1)
- Medidas de seguridad administrativa (2)
- Medidas de seguridad técnica (3)

### a) Atención de amenazas en el ámbito de los sistemas tecnológicos:

**Utilización de firewall tanto en equipos de cómputo como de seguridad perimetral adecuados.** A corto plazo, la Dirección de Informática y Estadística, mantendrá el monitoreo a las redes de seguridad donde se encuentren conectados los equipos de cómputo del organismo. (3)

**Utilización de Software antivirus.** A corto plazo, la Dirección de Informática y Estadística, mantendrá la supervisión de los antivirus instalados en equipos de cómputo, de manera especial en los que se resguarden sistemas de datos específicos, (con Sistemas de Datos Personales de nivel de protección "alto"). Las áreas deberán notificar a la Dirección, cualquier aviso o anomalía detectada en sus equipos de cómputo para que éste pueda ser atendido. (3)

**Establecimiento de contraseñas seguras de cambio periódico.** A corto plazo, todas las áreas del organismo deberán contar con contraseñas seguras en sus equipos de cómputo, así como de acceso a sistemas informáticos o bases que contengan datos. Para que una contraseña se considere segura, deberá contener por lo menos 8 dígitos conformada con letras, números y símbolos. Cada área determinará la periodicidad de actualización; no obstante, se sugiere

establecer como mínimo un cambio cada seis meses y de forma obligatoria, cuando haya cambios de personal. (3)
Adicional a lo anterior, se recomienda resguardar de forma apropiada las contraseñas asignadas, evitando tenerlas a la vista en post-it, compartirlas con el personal, etc.

Limitar descargas y accesos a sitios desconocidos. A corto plazo, todo el personal de las áreas del organismo debe abstenerse de descargar programas y/o softwares sin consentimiento de la Dirección de Informática y Estadística, así como accesos a sitios desconocidos. Asimismo, se recomienda no abrir hipervínculos de cuentas desconocidas que lleguen a las cuentas institucionales. (2)

Control de registros auditables de acceso a sistemas o bases que contengan datos personales. A corto plazo, la Dirección de Informática y Estadística, mantendrá la revisión de las consultas de información en el sistema de gestión de solicitudes de intervención, a fin de determinar accesos no autorizados. (3)

Implementación de softwares que permitan identificar intrusos o robos cibernéticos. A largo plazo, la Dirección de Informática y Estadística se encargará de la implementación de softwares adecuados para la identificación de intrusos en las redes del Organismo. Lo anterior, se sujetará a la disponibilidad presupuestal del mismo. (3)

Bitácoras de realización de copias de respaldo. A corto plazo, la Dirección de Informática y estadística deberá mantener el registro de la realización de copias de respaldo de la información que se encuentra en la nube en el Organismo a fin de mantener un control sobre su realización y advertir posibles fallas.

Todas las áreas que no formen parte de los servicios de la nube en el organismo, deberán establecer un procedimiento para la realización de sus propias copias de respaldo de información y en su caso, la implementación de la bitácora. Las asesorías que puedan requerirse al respecto podrán coordinarse con la Dirección de Informática y Estadística. (2)

Utilización de cuentas de correo oficiales o de uso oficial y abstenerse del uso de correos personales. A corto plazo, todas las áreas del organismo deberán abstenerse del uso de correos personales. Las comunicaciones oficiales se realizarán solo a través de correos institucionales. Los correos creados para “uso oficial” solamente podrán ser utilizados para comunicaciones internas. (2)

Utilizar dispositivos de almacenamiento institucionales (no utilizar memorias personales). A corto plazo, todas las áreas del organismo deberán disponer de memorias USB para el uso y manejo de información institucional, conforme a las necesidades de cada área. En caso de no contar con alguna, deberán solicitarla, a la Dirección de Administración conforme corresponda, a fin de dar cumplimiento a la política. (2)

Para el caso de prestadores de servicio social, las áreas deberán prever la disponibilidad de una memoria USB en la que puedan almacenar y/o compartir los archivos trabajados, a fin de evitar la utilización de dispositivos personales. (2)

### b) Atención de amenazas del entorno físico:

Implementación de sistemas de alarma contra incendios. A largo plazo, la Dirección de Administración, analizará la viabilidad de instalar sistemas de alarmas para prevenir incendios en las oficinas centrales del organismo, dando prioridad a los perímetros con mayor riesgo. (1)

Procurar la digitalización de expedientes. A largo plazo, la Dirección de Administración, la Secretaría Ejecutiva y la Unidad de Archivos en el ámbito de sus competencias, establecerán las directrices para promover la digitalización de la información generada por las áreas en el ejercicio de sus funciones y atribuciones, con la finalidad de contar con un respaldo y que se permita la gestión y consulta documental integral. (3)

Asignación y mantenimiento de extintores, así como brindar capacitación en su uso. A corto plazo, la Dirección de Administración mantendrá como medida preventiva, la asignación de extintores y prever la realización de acciones de capacitación, entrenamiento, formación e insumos necesarios al personal del organismo para el manejo de extintores. (2)

Uso correcto de reguladores de voltaje e implementación de revisiones preventivas. A corto plazo, las áreas deberán revisar el uso correcto de reguladores y la colocación de aparatos eléctricos evitando colocarlos cerca de expedientes o documentos para los que representen un riesgo en su integridad.

De forma simultánea, el Departamento de Recursos Materiales y Servicios Generales mantendrá revisiones periódicas para detectar deficiencias o mal uso en los reguladores asignados, estado de instalaciones eléctricas y/o adecuación de perímetros. De manera corresponsable, las áreas deberán informar a dicho Departamento sobre anomalías detectadas en sus áreas para que sean atendidas. (1)

Establecimiento de protocolos de atención de incidentes (en conjunto con el Comité de Protección Civil del Organismo). A mediano plazo, el Órgano Interno de Control, proporcionará un documento detallado como propuesta a la Dirección de Administración, con la finalidad de que este sea revisado y en su caso, implementado de manera adicional a los esfuerzos del Comité de PC. (2)

Adecuación de espacios en Delegación Zongolica. A corto plazo, de forma preventiva se solicitó el resguardo de expedientes activos solo en el cajón superior del archivero. Adicionalmente se deberá digitalizar los expedientes en trámite como respaldo adicional ante la posible materialización de una amenaza derivada del entorno físico.

La información digitalizada, será considerada de apoyo informativo ya que el trámite y turno de expedientes originales, continuará de forma ordinaria. Por lo anterior, para su conservación y eliminación deberán seguirse las reglas de archivo que le resulten aplicables.

A fin de que la Delegación pueda cumplir con la medida de seguridad, a mediano plazo, la Dirección de Administración, deberá dotarles de un disco duro externo con la capacidad suficiente para el resguardo de información digital. Para tal cumplimiento, la Dirección de Informática y Estadística, señalará las características idóneas mínimas que tal dispositivo de almacenamiento digital requiere previo a la adquisición. (1)

Atención de casos de humedad u otras reparaciones de oficinas. A mediano plazo, la Dirección de Administración deberá dar atención a los reportes de humedad en las instalaciones del Organismo señalados en las áreas que se ubican en oficinas centrales. Adicionalmente, de forma preventiva, las áreas que hayan detectado humedad, deberán prever la ubicación de documentos en zonas en donde haya menos humedad. (1)

Los casos de humedad y/o cualquier otra reparación o adecuación que se considere necesaria en las oficinas de las Delegaciones Étnicas y Regionales (por ejemplo, reforzar puertas, ventanas, etc.), deberán ser solicitados a los correspondientes arrendatarios por la

misma Delegación e informar a la Dirección de Administración sobre las peticiones realizadas y lo que resulte de tales solicitudes. (1)

Adquisición de archiveros y/o mejoramiento de espacios de almacenamiento. A mediano plazo, las áreas que requieran archiveros o mejorar espacios de almacenamiento para mantener el control de la documentación bajo llave, deberán informar a la Dirección de Administración sus necesidades. Dicha Dirección inspeccionará y evaluará la utilidad de los espacios físicos y su viabilidad para adquirir, reparar o reemplazar estos.

La reparación de espacios y mobiliarios que hayan sido solicitados por las áreas serán atendidos por la Dirección de Administración conforme corresponda. En todo caso, las áreas son corresponsables de dar seguimiento a las reparaciones solicitadas. Adicionalmente, la Dirección podrá analizar la viabilidad para reorganizar espacios entre las áreas o reubicaciones de áreas administrativas que lo requieran, con la finalidad de optimizar el uso de perímetros. (1)

Dotar a las áreas de los artículos de oficina necesarios para el cumplimiento de las medidas de seguridad. A corto plazo, las áreas con necesidades específicas deberán solicitar o reiterar por escrito a la Dirección de Administración, sus peticiones de artículos necesarios para mantener las medidas de seguridad establecidas por el SGS. Cuando la suficiencia presupuestal lo permita, la Dirección de Administración, proporcionará los artículos solicitados. (1)

Se consideran artículos necesarios para mantener las medidas de seguridad los siguientes:

- Trituradoras, para garantizar la correcta destrucción de borradores u otros documentos cuando proceda.
- Foliadores, para el correcto foliado de expedientes conforme corresponde.
- Grabadoras, para el correcto tratamiento y resguardo de las entrevistas necesarias para la emisión de dictámenes de valoración de impacto.
- Discos de almacenamiento externo, para la correcta realización de copias de respaldo o digitalización, en las áreas cuyo análisis de riesgo lo determinó necesario.

Mantener la documentación en espacios de almacenamiento seguros bajo llave. A mediano plazo, la Dirección de Administración preverá la colocación de la puerta de entrada al piso

donde se ubica la Dirección de Orientación y Quejas a fin de reforzar la seguridad perimetral de la documentación de las áreas ubicadas en el mismo.

Al respecto, las áreas de cada piso serán corresponsables de verificar que, al retirarse de la jornada laboral, dichas puertas de acceso queden cerradas. DOQ. (1)

**Establecer medidas administrativas de organización y control de documentos entre áreas ubicadas en un mismo piso.** A mediano plazo, la Secretaría Ejecutiva y la Dirección de Administración, deberán establecer los canales de comunicación con las Direcciones de Atención a Víctimas y Grupos en Situación de Vulnerabilidad y Asuntos Penitenciarios, con la finalidad de coordinar reglas de interacción entre el personal que contribuyan a mantener el correcto control y orden documental. (2)

### c) Atención de amenazas del entorno organizacional:

**Establecer procedimientos de control de acceso a las instalaciones.** En el corto plazo, tratándose de oficinas centrales, la Dirección de Administración deberá retomar el control de acceso mediante el uso de gafetes que permitan identificar tanto a prestadores de servicio social y visitantes, a fin de poder advertir su acceso a áreas no autorizadas.

A mediano plazo, la Dirección de Administración analizará la viabilidad de retomar el proyecto de asignación de gafetes a las personas servidoras públicas del Organismo, como una medida de identificación para fortalecer la seguridad. Para el cumplimiento de lo anterior, la Secretaría Ejecutiva y la Dirección de Informática y Estadística, serán corresponsables de conformidad con sus atribuciones. (1)

Para el control de acceso en las Delegaciones, éstas podrán determinar el control a aplicar, procurando evitar la recopilación excesiva de datos personales y procesos complejos de registro. En caso de que sus instalaciones permitan mantener las protecciones de entrada cerradas como un método de control de acceso, podrán mantener dicha disposición, siempre que se establezcan medidas para garantizar el fácil y rápido acceso de los usuarios a las instalaciones, evitando causar molestias a estos. (1)

**Establecimiento de bitácoras y registros.** A corto plazo, todas las áreas del organismo, deberán establecer una bitácora de acceso a expedientes o bases de datos, en la cual se

deberá registrar el nombre de las personas servidoras públicas que reciben y autorizan la consulta, la fecha de consulta, el expediente o documento a consultar y un apartado de observaciones para registrar cualquier anomalía detectada en el momento de la consulta. Lo anterior con la finalidad de mantener el control de las documentales que conforman un expediente y reconocer posibles accesos no autorizados o vulneraciones a los documentos.

Adicionalmente, todas las áreas del organismo, deberán mantener un registro de vulneraciones, en el que se deberán registrar aquellos incidentes que constituyan una vulneración de seguridad.

De forma paralela, en caso de que ocurra una vulneración de seguridad, el área donde ocurrió deberá el llenar la bitácora de vulneraciones, para los detalles del incidente ocurrido, y estar de condiciones de rendir el informe que establece el Plan de Respuesta a Vulneraciones. (2)

Establecimiento de procedimientos de revisión periódica de documentos. A corto plazo, todas las áreas que integran expedientes de solicitudes de intervención deberán establecer un procedimiento de revisión periódica de sus expedientes, que comprenda el cotejo físico y electrónico, con la finalidad de evitar pérdidas, fugas o malos manejos de la documentación que contienen.

Para lo anterior, cada área definirá la periodicidad en que se llevará a cabo, en tal caso, se recomienda no exceder de un periodo de tres meses. El cumplimiento de dicha medida deberá informarse a la Unidad de Transparencia y al Órgano Interno de Control, este último con la finalidad de que brinde acompañamiento en su realización conforme a sus atribuciones. (2)

Resguardo de información ante ataques a las instalaciones. Con relación al protocolo de atención de incidentes que propondrá el OIC en colaboración con la Dirección de Administración y el Comité de PC, la Unidad de Transparencia, emitirá recomendaciones para la custodia y preservación de la información en posesión del organismo que se deben considerar ante la amenaza de un ataque a las instalaciones que ponga en peligro la integridad de la documentación en posesión del Organismo. (2)

Medidas preventivas de incidentes ajenos al Organismo. A corto plazo, todas las áreas del organismo, deberán mantener la utilización de la leyenda de mensajería de la CEDHV

establecida para la protección de datos: *"La documentación adjunta puede contener datos personales recabados y protegidos de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz por la Comisión Estatal de Derechos Humanos y está dirigida exclusivamente a su destinatario. Si usted la recibe por error, le rogamos nos lo comunique al teléfono 800 260 22 00 y proceda a su resguardo o de no ser posible, a su destrucción."*
Dicha leyenda será de uso obligatorio para rotular los sobres de paquetería a través de los cuales se envíen documentos oficiales. (2)

### d) Atención de amenazas del entorno personal:

**Control de funciones del personal, con base en el formato de funciones y obligaciones del SGS.** A corto plazo, todas las áreas del organismo, deberán conservar la información actualizada del nombre de la base de datos, sistema o archivo que tenga datos personales con relación a el servidor público, respectivo cargo, funciones y obligaciones, así como el fundamento que faculte a tal acción administrativa conforme el formato de actualización del SGS.

El acceso a expedientes o bases de datos, deberá realizarse en concordancia a las facultades y atribuciones de cada servidor público a través de las credenciales de acceso proporcionadas. (2)

**Establecimiento de políticas de confidencialidad y aplicación de sanciones.** A corto plazo, todas las áreas del organismo están obligadas a mantener la confidencialidad de la información a la que tienen acceso conforme a sus atribuciones, respetando los principios y deberes de la protección de datos personales y estableciendo las medidas de seguridad que les correspondan conforme a las presentes políticas. En caso de no acatarse se estará a las sanciones que correspondan conforme las políticas establecidas y en su caso, el Reglamento Interno de esta Comisión. (2)

**Resguardo y/o traslado de datos recopilados en diligencias fuera del Organismo**. A corto plazo, las áreas sustantivas del organismo, deberán implementar la recolección y resguardo de los datos obtenidos en diligencias realizadas fuera de las instalaciones de la Comisión (oficinas centrales o delegaciones) en un periodo máximo de 24 horas a partir de su recolección. Si la Diligencia y distancia lo permite, la persona servidora pública que los haya recabado, deberá remitirlos a la oficina que le corresponde a la brevedad para su respaldo

en los archivos del Organismo, a fin de evitar posibles alteraciones en los datos, afectaciones a la información recabada por dispositivos dañados o extraviados, etc.

En caso de que, por el tipo de diligencia y periodo de duración, no sea posible cumplir con lo anterior, la información recopilada deberá constar en el respaldo de archivos del área que corresponda inmediatamente al retorno del visitador o persona que los haya recabado. (2)

Homologación de un proceso de verificación de identidades. Tratándose de información consultada vía telefónica, en el corto plazo, las áreas sustantivas del organismo deberán homologar un procedimiento de seguridad para acreditar la identidad de las personas que dicen ser parte de un expediente en el organismo, a través de preguntas de seguridad o solicitud de datos personales. Las áreas de común acuerdo establecerán los datos a requerir, de conformidad con su viabilidad.

Lo anterior, con la finalidad de tener la certeza de que la persona a quien se brinde información vía telefónica es parte del procedimiento l que solicita el acceso (2).

Capacitación a los servidores públicos. En materia de responsabilidades y sanciones, desde el corto al largo plazo, la Unidad de Transparencia propondrá cursos de capacitación, desde un diseño propio o con la doctrina de un órgano garante, dirigido a los servidores públicos del organismo. Además, para las materias de "Ética pública, uso ilícito de atribuciones y facultades", podrá solicitar la colaboración del Órgano Interno de Control de este organismo.

En materia de conservación, manejo y baja de archivos (prácticas de cuidado adecuado de documentos, desde el corto al largo plazo, se analizarán las ofertas de capacitación en la materia para fortalecer el conocimiento entre los servidores públicos del organismo sobre la administración de documentos. Para lo anterior, la Unidad de Transparencia solicitará la colaboración de la Unidad de Archivos de este organismo.

En materia de principios y deberes de la protección de datos personales, desde el corto al largo plazo, la Unidad de Transparencia propondrá capacitación, desde un diseño propio o con la doctrina de un órgano garante, dirigido a los servidores públicos del organismo.
Las ofertas de cursos de capacitación, serán enviadas con oportunidad a las áreas para su consideración. (2)
Implementación obligatoria de medidas de seguridad y monitoreo de su cumplimiento. Las políticas enlistadas son de cumplimiento obligatorio para todas las áreas del organismo de

conformidad con los riesgos y amenazas detectados. Por lo anterior, es responsabilidad de los titulares, dar a conocer los deberes, obligaciones, medidas de seguridad a implementar y en su caso, las sanciones aplicables que contienen las presentes políticas internas para que sean del conocimiento y aplicación de todo el personal a su cargo, prestando especial atención en aquellos de nuevo ingreso.

El cumplimiento de las políticas internas deberá ser monitoreado por cada área a fin de asegurar su cumplimiento, para lo cual se pueden auxiliar de sus respectivos responsables de seguridad (cuando correspondan). Asimismo, la Unidad de Transparencia podrá llevar a cabo acciones de monitoreo y verificación del cumplimiento de las políticas establecidas, para lo cual podrá auxiliarse del Órgano Interno de Control del Organismo. (2)

Recomendaciones Generales del Trabajo a distancia. Las áreas que cuenten con personal trabajando a distancia, deberán asegurarse de implementar medidas de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información que contiene datos personales, en entornos externos a las oficinas del Organismo. Para lo anterior pueden considerarse como mínimo las siguientes:

- Evitar conectarse en redes públicas o de acceso gratuito con el equipo habilitado para el desarrollo de actividades laborales.
- Cuidar que, el entorno en que se realizará el tratamiento de datos personales, sea un espacio seguro, adecuados, alejados de aparatos que puedan comprometer su integridad.
- Generar copias de respaldo de toda la documentación generada fuera el perímetro institucional para evitar pérdidas de información que no cuenten con respaldo.
- Llevar una bitácora de los documentos trasladados a espacios externos y registrar cualquier incidente que pueda causar una afectación a los mismos.