COMISIÓN ESTATAL DE
DERECHOS HUMANOS
VERACRUZ

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

Edición 2021

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.

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, así como para las y los Encargados de los Datos de la CEDH.

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.

PROCESO DE MONITOREO Y EVALUACIÓN

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 anual 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.

17. Evaluación

La evaluación de las medidas implementadas se realizará a través de procedimientos de Auditoría Anuales o Semestrales realizadas por 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.

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

MEDIDAS DE SEGURIDAD APLICABLES EN LA CEDHV

ARTICULO 43 LPDPPSOV

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. • Sistema de Datos de las Organizaciones de la Sociedad Civil. • Sistema de Datos Personales de los Expedientes de Solicitudes de Acceso a la Información y Derechos ARCO de la CEDH Veracruz. • 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. • Sistema de Datos Personales de Registro de Periodistas y Medios de Comunicación de la CEDH Veracruz. • Sistema de Datos Personales de las Redes Sociales de la CEDH Veracruz. • Sistema de Datos Personales de la Recopilación de Evidencias de las Actividades de la CEDH Veracruz. • Sistema de Datos Personales del Registro de Asistencia a Eventos de la Unidad de Atención a Niñas, Niños y Adolescentes. • Sistema de Datos Personales del Registro de Asistentes a Reuniones de Trabajo y Vinculación de la Secretaría Ejecutiva de la CEDH Veracruz.	Medidas Mínimas Físicas, Técnicas y Administrativas	A a la G
Medio	• Sistema de Datos Personales de los Recursos Humanos. • Sistema de Datos Personales de los Expedientes de los Prestadores del Servicio Social. • 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. • Sistema de Datos Personales del Padrón de Proveedores de la Comisión Estatal de Derechos Humanos Veracruz. • Sistema de Datos Personales de Resolución del Recurso de Revocación de la Comisión Estatal de Derechos Humanos de Veracruz. • Sistema de Datos Personales de Responsabilidades, Faltas Administrativas, Quejas y Sanciones de los Servidores Públicos de la Comisión Estatal de Derechos Humanos de Veracruz. • Sistema de Datos Personales de Denuncias ante la Fiscalía Especializada en Combate a la Corrupción de la Comisión Estatal de Derechos Humanos de Veracruz. • Sistema de Datos Personales de las Actividades de la Unidad para la Igualdad de Género. • Sistema de Datos Personales del Monitoreo de Albergues para Migrantes. • 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.	Medidas Mínimas Físicas, Técnicas y Administrativas	A a la K

Alto	• Sistema de Datos Personales de solicitudes de intervención, quejas, recursos y seguimiento de resoluciones • Sistema de Datos Personales de Asistencia a Víctimas para su Incorporación al Registro Estatal de Víctimas por parte de la CEDH Veracruz. • Sistema de Datos Personales de Entrevistas para la Emisión de Dictámenes de Valoración de Impacto y aplicación de Protocolos de Estambul de la CEDHV. • 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 Responsable de los Sistemas de Datos deberán implementar las medidas de seguridad que de acuerdo al nivel le correspondan y de conformidad con los controles establecidos en el Sistema de Gestión, con base en lo siguiente:

CATEGORÍA DE MEDIDAS

Medidas De Seguridad Físicas y Ambientales

Para la seguridad física y del entorno, las medidas de seguridad que se establezcan en cada perímetro y sobre los archivos con datos personales deben ser proporcionales a los riesgos declarados por cada área Responsable e identificada por la Unidad de Transparencia. Para que un Área Administrativa considere viable acondicionar un espacio físico para resguardar el material documental y/o bases de datos, se debe procurar su instalación en áreas seguras y perímetros definidos mediante accesos de seguridad y controles de entrada adecuados, considerando además lo dispuesto en la Ley General de Archivos que resulte aplicable.

Medidas de Seguridad Técnicas. 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.
- Control de acceso.
- Adquisición, desarrollo, uso y mantenimiento de sistemas de información.

Medidas de Seguridad Administrativas

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

- Política de seguridad.
- Cumplimiento de la normatividad.
- Organización de la seguridad de la información.
- Clasificación y control de activos.
- Seguridad relacionada a los recursos humanos.
- Administración de incidentes (vulneraciones).

- Continuidad de las operaciones.

A. TIPOS DE SEGURIDAD

Las medidas de seguridad físicas, técnicas o administrativas pueden referir a los siguientes tipos de seguridad:

I. Física
II. Lógica
III. De desarrollo y aplicaciones
IV. De cifrado
V. De comunicaciones y redes

(Consultar Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de los Datos Personales en la CEDHV).

Su implementación, se realizará atendiendo al catálogo de recomendaciones de medidas de seguridad mínimas establecidas y la matriz de controles señaladas en los Anexos I.1 y I.2.

B. NIVELES DE SEGURIDAD

I. **Básico.** Medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales.
Le serán aplicables las medidas de la a) a la g).

II. **Medio.** Medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, contempla medidas adicionales a las medidas calificadas como básicas.
Le serán aplicables las medidas de la a) a la i)

III. **Alto.** Medidas de seguridad aplicables 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. Incorpora medidas adicionales a las medidas de nivel básico y medio.
Le serán aplicables las medidas de la a) a la n)

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 II.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 II.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 III)

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 IV

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 V

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 VI

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 VII

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

I. Medidas de Seguridad y Controles:

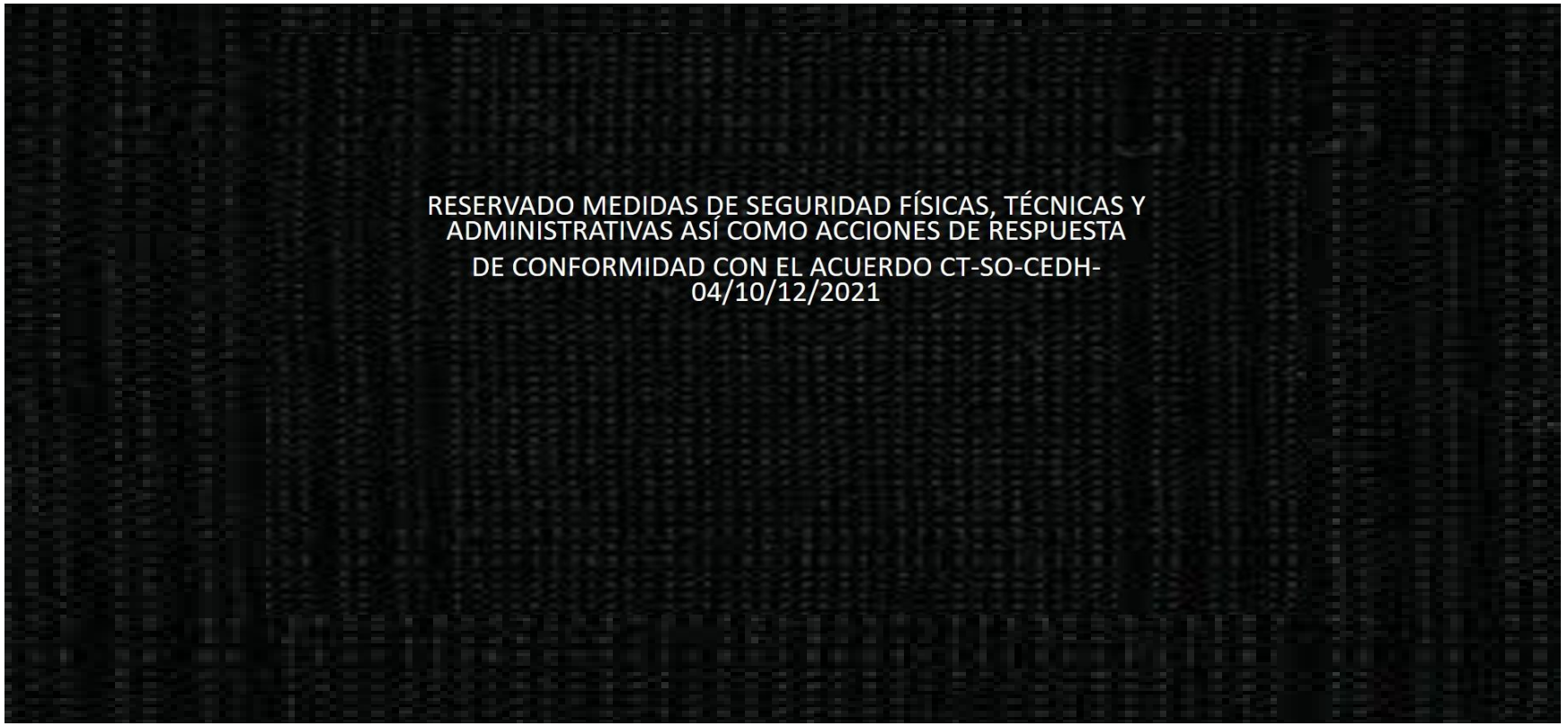
COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ




RESERVADO MEDIDAS DE SEGURIDAD FÍSICAS, TÉCNICAS Y ADMINISTRATIVAS ASÍ COMO ACCIONES DE RESPUESTA
DE CONFORMIDAD CON EL ACUERDO CT-SO-CEDH-04/10/12/2021

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo II.1 Formato de Registro de Vulneraciones

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

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo II.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 ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada ☐	
ORIGEN	Interno ☐ Externo ☐	
CATEGORÍA DE DATOS COMPROMETIDOS	☐ Identificativos ☐ laborales ☐ Académicos ☐ electrónicos ☐ De la salud ☐ patrimoniales ☐ Sobre procedimientos administrativos ☐ De tránsito o movimientos migratorios ☐ Sensibles. Especifique: _____	
VOLUMEN Y CATEGORÍA DE AFECTADOS	Número de afectados: _____ Categoría (servidores públicos, víctimas, quejosos, etc.): _____	

<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>_____
NOMBRE Y FIRMA DE QUIEN REPORTA</td><td>_____
NOMBRE Y FIRMA DE QUIEN ADMINISTRA EL SISTEMA</td><td>_____
NOMBRE Y FIRMA DEL TITULAR DEL ÁREA</td></tr>
</table>

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo III. **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

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo IV **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)

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo V. **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 VI **Formato para la designación de responsable de seguridad**

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 de Sistemas de Datos Personales.

En cumplimiento a lo anterior, hago de su conocimiento que en mi calidad de responsable de dicho Sistema, se le designa como responsable de seguridad del sistema de datos _____, a cargo de (área) _____ de la que usted forma parte.

Para el cumplimiento de su encargo, deberá llevar a cabo las funciones establecidas en el documento de seguridad de la CEDH Veracruz, específicamente para dar seguimiento y coordinar al interior de su área, las medidas de seguridad aplicables al sistema que les corresponde.

(saludo)…

Atentamente

(Nombre y firma del titular) _____

(Cargo) _____

Con copias de conocimiento y efectos

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

Anexo VII **Formatos del Proceso de Auditoría**

VII.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) (Unidad de Trasparencia)	Visto bueno (13) (Contraloría Interna)	Autorizó (14) (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 Cronograma de Actividades a Desarrollar										
No.	Actividad	T. Estimado	T. Real	(Calendario de días)						
_____ Elaboró (personal UT)			_____ Vo.Bo. (Personal C.I.)				_____ Autorizó (Personal C.I.)			
Iniciales T. Estimado: Tiempo estimado para la auditoría 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 _____

VII. 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.

COMISION ESTATAL DE DERECHOS HUMANOS VERACRUZ

VII. 5. **Procedimiento de Auditoría**

Sujeto Obligado:	Número de auditoría:
Área administrativa Auditada: ----------	Sistema de Datos Personales:
Tipo de Auditoría: AUDITORÍA INTERNA	Objetivo de la Auditoría: 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: Artículos 38, fracción V, 43 al 56, 58 y 59 de la Ley PDPPSOEV	R						

P = Programado

R = Real

Elaboró
(Personal UTR)
_____

Revisó
(Personal C.I.)
_____

Autorizó
(Personal C.I.)
_____

ACUERDO CT-SO-CEDH-04/10/12/2021 DE LOS INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN ESTATAL DE DERECHOS HUMANOS DE VERACRUZ, POR EL QUE SE APRUEBA EL DOCUMENTO DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA COMISIÓN ESTATAL DE DERECHOS HUMANOS, Y EL CALENDARIO DE SESIONES ORDINARIAS 2022 DEL COMITÉ DE TRANSPARENCIA, AL TENOR DE LOS SIGUIENTES:

CONSIDERANDOS

I. Que el día tres de octubre de dos mil dieciséis, se constituyó el Comité de Transparencia de esta Comisión Estatal de Derechos Humanos, en Sesión Ordinaria, quedando asentado mediante ACTA-CIAR04-03-10-2016, a cuyos integrantes se les otorgaron las atribuciones contenidas en el actual Capítulo III, del Título V, de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave.

II. Que de conformidad con lo ordenado por los artículos 131 fracciones I y II, 150 fracción II y 151 de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, compete al Comité de Transparencia la declaración de inexistencia, clasificación, declaración de incompetencia o ampliación del plazo, respecto de la información requerida a través de las solicitudes de información así como cualquier otra decisión relacionada con la información que genera la Comisión Estatal de Derechos Humanos.

III. Que en cumplimiento a los artículos 47 y 48 de la Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave, la Unidad de Transparencia presentó a este Comité de Transparencia la propuesta de Documento de Seguridad del Sistema de Gestión de Seguridad elaborado con base en los requisitos señalados en el artículo 48 de la Ley 316 antes citada para su validación por parte de este Órgano colegiado.

IV. Que al haber recibido el Comité de Transparencia, la propuesta en los términos que anteceden; este Comité, es legalmente competente para validar su aprobación, de conformidad con los preceptos legales antes citados y sus correlativos de la Ley General de Transparencia y Acceso a la Información Pública.

Por las razones que anteceden, el Comité de Transparencia en seguimiento a lo acordado en su Cuarta Sesión Ordinaria de fecha diez de diciembre de dos mil veintiuno, emite el siguiente:

ACUERDO

PRIMERO.- De conformidad con el artículo 47 de la Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados, las acciones realizadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un Sistema de Gestión. Éste deberá entenderse como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Asimismo, el artículo 48 de la misma Ley establece que es obligación de los encargados y demás personas que participan en el tratamiento de datos personales, contar con un "Documento de Seguridad", el cual debe contener los siguientes elementos:

"… I. Respecto de los sistemas de datos personales:
a) El nombre;
b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos;

c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales;
d) El folio del registro del sistema y base de datos;
e) El inventario o la especificación detallada del tipo de datos personales contenidos, y
f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan;

II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:
a) El inventario de datos personales y de los sistemas de tratamiento;
b) Las funciones y obligaciones de las personas que traten datos personales;
c) El análisis de riesgos;
d) El análisis de brecha;
e) El plan de trabajo;
f) Los mecanismos de monitoreo y revisión de las medidas de seguridad;
g) El programa general de capacitación; y
h) La relación de personas autorizadas para dar tratamiento a los datos personales, así como los permisos y derechos de acceso…"

En cumplimiento a lo anterior, en la Décimo Octava Sesión Extraordinaria del año 2021 de este Comité celebrada el 27 de octubre de 2021, la Unidad de Transparencia sometió a aprobación de este Órgano el Plan de Trabajo para la actualización del Sistema de Gestión de Seguridad de Datos Personales de la CEDH.

En ese sentido, la Unidad de Transparencia en colaboración con las áreas administrativas de este Organismo desarrollaron los documentos que la Ley 316 establece para conformar el Documento de Seguridad, mismo que presenta ante este Comité para su aprobación. En cumplimiento a lo establecido por el artículo 48 antes referido, el Documento de Seguridad presentado por la Unidad de Transparencia contempla los siguientes apartados:

- Introducción y marco normativo.
- El Programa de actualización del Sistema de Gestión.
- Respecto de los Sistemas de datos personales: nombre del sistema, nombre, cargo y responsable del sistema, folio de registro electrónico, funciones y obligaciones, inventario de datos y bases de datos y tipo de soporte.
- Respecto a las Medidas de Seguridad implementadas:
  - El inventario de datos personales, que contiene la relación de tipos de datos que se recaban por áreas, nombre y cargo de los servidores públicos que realizan el tratamiento, medios de obtención, finalidades del tratamiento, tipo de tratamiento realizado, instrumento jurídico que faculta, la forma de almacenamiento y transferencias realizadas. (Fracción I incisos c), e) y f), del art. 48). Así como el inventario general por categoría.
  - El catálogo de identificación de funciones y obligaciones que contiene por cada Sistema de Datos Personales y área que trata, lo siguiente: El sistema a que tiene acceso, los servidores públicos responsables del sistema y los usuarios del sistema, así como funciones y obligaciones de éstos. (Fracción II incisos a) y b), y h) del art. 48).
  - El análisis de riesgo y el análisis de brecha, que en su conjunto contienen: el riesgo por el valor cuantitativo o cualitativo de los datos (matrices que establecen la clasificación de la brecha, el activo, tipo de amenaza, riesgo, la probabilidad de ocurrencia y el nivel de seguridad de los datos), así como las medidas establecidas para su tratamiento. (Fracción II inciso c) del art. 48).
  - El plan de trabajo, en el cual se estableció la prestación de los instrumentos desarrollados tanto al equipo de trabajo conformado como a los titulares de las áreas administrativas, la identificación de

metas a corto, mediano y largo plazo para el cumplimiento del Sistema de Gestión, las Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de los Datos Personales en la CEDH y las medidas de seguridad aplicables por nivel de protección, los procedimientos de control y seguimiento, el programa de capacitación y el cronograma de implementación. (Fracción II inciso e), del art. 48).

- Mecanismo de monitoreo: Los resultados del procedimiento de verificación inicial llevado a cabo. (Fracción II inciso f) del art. 48).

Teniendo a la vista los anteriores documentos y una vez revisado su contenido, este Comité ha constatado que el documento presentado por la Unidad de Transparencia cumple con los requisitos establecidos en el artículo 48 de la Ley, tal como se ha relacionado con los números que anteceden.

Siendo así, con fundamento en el artículo 116 fracciones I, II y VI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, este Comité **aprueba por unanimidad de votos** de sus integrantes, Licenciada Minerva Regina Pérez López, Licenciado Miguel Ángel Córdova Álvarez y Licenciada Sandra Jazmín Velasco Toto, la Primera en su carácter de Presidenta y los demás en su carácter de Vocales, el contenido del "Documento de Seguridad" de la CEDHV Veracruz, mencionado en el considerando **TERCERO**.

SEGUNDO.- Se instruye a la Titular de la Unidad de Transparencia para que informe al Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales respecto a la aprobación del "Documento de Seguridad de la CEDHV" y remita en su caso, la versión pública del mismo para lo cual deberán testarse los datos siguientes:

- Del inventario de datos personales (anexo electrónico): Nombre y cargo del personal que tiene acceso a cada sistema y las observaciones detectadas.
- Del catálogo de identificación de funciones y obligaciones (anexo electrónico): nombre y cargo de los usuarios de cada sistema.
- De las medidas de seguridad: la identificación de la seguridad aplicada al tratamiento de datos personales.
- Del análisis de riesgo: la descripción de los riesgos, probabilidad, valor cuantitativo y cualitativo, gravedad, calificación, nivel de riesgo y el tratamiento o control operacional.
- Del análisis de brecha: Tipo de medida. Existencia, tipo de seguridad, operatividad, deficiencia y observaciones.
- Del Plan de Trabajo: las metas a corto, mediano y largo plazo; el procedimiento de seguimiento y control, el cronograma de implementación.
- De las políticas internas y medidas preventivas: las medidas físicas, técnicas y administrativas, así como las acciones de respuesta que las áreas administrativas implementarán al interior de la Comisión Estatal de Derechos Humanos para garantizar la protección de los datos personales.
- De los resultados de procedimiento y control: el nombre y áreas verificadas, los resultados de la auditoría, las variables, el valor general y el resultado general, observaciones, buenas prácticas y recomendaciones.

Todo lo anterior, con fundamento en lo dispuesto por el artículo 113 fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, 68 fracción II de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz, así como Décimo Octavo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información así como para la Elaboración de Versiones Públicas, los cuales establecen que puede clasificarse como reservada aquella información que comprometa la seguridad pública o pueda poner en peligro las funciones a cargo de del orden público u obstruya las actividades de verificación, inspección o auditoría relativas al cumplimiento de las leyes.

En ese orden de ideas, la implementación de un Sistema de Gestión para la seguridad de los datos personales de Acuerdo con la Ley 316 de Protección de Datos Personales tiene como objetivo prevenir posibles vulneraciones a la seguridad de los datos y establecer las medidas físicas, técnicas y administrativas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información en posesión de los sujetos obligados. Por su parte el Documento de Seguridad recopila todas estas medidas y controles establecidos en dicho Sistema y señala directamente a los servidores públicos que con motivo de sus funciones tienen acceso a determinados datos de particulares, el estado físico y de conservación en que se encuentran, los controles de seguridad, etc.

Revelar la anterior información, implica poner a disposición de la ciudadanía información que puede comprometer el desarrollo de las funciones que este Organismo realiza, así como revelar las posibles rutas de acceso que un particular con intenciones no legítimas podría seguir para lograr el acceso a determinados datos personales, lo cual por sí mismo generaría una amenaza y un riesgo de vulneración de los mismos. Aunado a lo anterior, el texto de la Ley 316 de Protección de Datos antes citada establece que es obligación de los responsables establecer dicho Sistema y conformar el Documento de Seguridad, mas no la obligación de hacerlo público a la ciudadanía.

En ese sentido, el Documento de Seguridad contiene los controles aplicados por el sujeto obligado para prevenir vulneraciones de seguridad (que en determinado momento pueden inclusive constituir delitos), por lo que su divulgación podría comprometer la eficacia de las medidas establecidas y la capacidad de respuesta de este Organismo ante una posible materialización de un riesgo. Siendo así, únicamente compete a los servidores públicos que forman parte de esta Comisión y que están involucrados en el tratamiento de datos personales conocer su contenido para efectos de llevar a cabo la implementación de las medidas.

Por lo anterior, se considera fundado y procedente clasificar en la modalidad de reservada la información señalada con anterioridad, para lo cual se presenta la siguiente prueba de daño:

Tipo de información: *"Documento de Seguridad de la CEDHV"*			***Rubro Temático:*** *Medidas para la seguridad y confidencialidad de los datos personales.*	
Presupuesto	***Prueba***	***Justificación***	***Resultado***	***Razones***
Información Reservada *"Documento de Seguridad de la CEDHV"*	*Prueba de daño*	*Ponderación* *Fin legítimo: Derecho de acceso a la información.* *Que la divulgación de la información comprometa la eficacia de las medidas establecidas y la capacidad de*	*Clasificación (X)*	*Daño MAYOR a la seguridad de los datos personales (X).* *Daño MAYOR a la eficacia de las medidas y capacidad de respuesta del sujeto obligado (X).*

		respuesta del organismo para atender la materialización de un riesgo. *Que la divulgación de la información revele las brechas a los que está expuesta la información, otorgando al público la posibilidad de acceder de forma ilegítima a los datos.* *Idoneidad y/o necesidad de la clasificación: La clasificación de la información es la medida idónea para garantizar el derecho a la protección de los datos personales.*	*Divulgación ( )*	*Daño MENOR al interés público(X)*
Causal aplicable:	*Artículo 72 fracciones I y III de la Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, 113 fracciones I y VII de la Ley General de Transparencia y Acceso a la Información Pública y Décimo Octavo y Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.*			
Clave de identificación: Ninguna	*Determinación: Se acuerda clasificar con la categoría de "Reservada", las medidas físicas, técnicas y administrativas, así como acciones de respuesta contenidas en las "Políticas Internas y Medidas Preventivas para la Gestión, Tratamiento y Protección de los Datos Personales en la CEDH Veracruz, hasta por un periodo de 5 años, resaltando que el acceso a dicha información corresponde únicamente a los servidores públicos facultados para ello.*			

TERCERO.- Con fundamento en el artículo 130 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, este Comité **aprueba por unanimidad de votos** de sus integrantes, Licenciada Minerva Regina Pérez López, Licenciado Miguel Ángel Córdova Álvarez y Licenciada Sandra Jazmín Velasco Toto, la Primera en su carácter de Presidenta y los demás en su carácter de Vocales, el calendario de sesiones ordinarias del Comité de Transparencia de la Comisión Estatal de Derechos Humanos de Veracruz para el ejercicio 2022, de acuerdo a lo siguiente.

NÚMERO DE SESIÓN	FECHA	HORA
1° Sesión Ordinaria	11 de marzo	10:00
2° Sesión Ordinaria	10 de junio	10:00
3° Sesión Ordinaria	9 de septiembre	10:00
4° Sesión Ordinaria	9 de diciembre	10:00

CUARTO.- El presente Acuerdo entra en vigor a partir de su aprobación.

QUINTO.- Se instruye a la responsable de la Unidad de Transparencia, para que proceda en los términos aprobados por este Comité, respecto al punto objeto de análisis.

SEXTO.- Publíquese este acuerdo en el Portal de Transparencia de esta Comisión Estatal, así como en la Plataforma Nacional de Transparencia, como corresponda según los lineamientos de la materia.

Dado en la Sala de Juntas de la Comisión Estatal de Derechos Humanos, en la ciudad de Xalapa-Enríquez, Veracruz, a los diez días del mes de diciembre de dos mil veintiuno.

LIC. MINERVA REGINA PÉREZ LÓPEZ
PRESIDENTA

LIC. SANDRA J. VELASCO TOTO
VOCAL

MTRO. MIGUEL A. CÓRDOVA ÁLVAREZ
VOCAL