PLAN DE CONTINGENCIA EN MATERIA PARA LA PROTECCION DE DATOS PERSONALES

PLAN DE CONTINGENCIA EN MATERIA PARA LA PROTECCION DE DATOS PERSONALES.

Presentación

En cumplimiento al artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas, el Comité del H. Congreso del Estado aprobó el Documento de Seguridad, mediante la celebración de la Trigésima Quinta Sesión Extraordinaria de fecha 2 de diciembre del 2022. Así como, tomando en consideración lo estipulado en los dispositivos 45, 46, 47, 48, 49, y 50, fracción XV, 113 y 114, fracciones I, VI y VII de la Ley de Protección de Datos Personales Local, la Unidad de Transparencia pone a consideración del Comité de Transparencia un Plan de Trabajo relacionado con el contenido del Documento de Seguridad del H. Congreso del Estado de Chiapas.

Que el plan de contingencias servirá para la protección de la información, a la definición de acciones a realizar, recursos a utilizar, y el personal a emplear en caso que se produzca un acontecimiento de carácter intencional o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos del H. Congreso del Estado. El Plan de Contingencia del H. Congreso del Estado, es un protocolo de actuación que servirá para atender las contingencias que se presenten eventualmente.

Clasificación de Contingencia:

De acuerdo al tipo de contingencia es posible determinar el grado de afectación.

Grado 1	Grado 2
• Son las más bajas que van desde fallas eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal de este H. Congreso del Estado.	• Son las contingencias provocadas por un siniestro y por su alcance pueden afectar severamente la operatividad del Poder Legislativo, por ejemplo una inundación o un incendio, en estos casos se requiere tanto del apoyo de personal del H. Congreso del Estado, como del Cuerpo de Bomberos y de Protección Civil Municipal o del Estado.

Integración del Plan de Contingencia:

El Plan de Contingencias deberá contener lo siguiente:

- Consideraciones principales
- Reporte de Vulneraciones
- Designación de Personas
- Investigación de la vulneración ocurrida
- Medidas de prevención y conservación de archivos
- Medidas preventivas ante los siguientes siniestros:
  - Incendio
  - Terremoto o sismo
  - Inundaciones
  - Robo
  - Huelga o Manifestaciones

- Amenazas informáticas (hackeo informático)

I. Consideraciones Principales:

- Se debe realizar una evaluación de los riesgos.
- Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Designación de un encargado de cada área administrativa y sirva de apoyo en cualquier desastre que ocurra y se genere una contingencia, los encargados recibirán capacitación para el manejo de las mismas, como por ejemplo: el uso de extintores, planes de evacuación, etc.
- Es necesario hacer las pruebas previas al Plan de Contingencia, para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).
- La brigada que se conforme estará integrada por cada uno de los encargados de las áreas administrativas.
- De las pruebas que se realicen, se llevarán reuniones con los encargados de las brigadas de las áreas administrativas
- Revisión del plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.

II. Reporte de Vulneraciones.

Para realizar el reporte de vulneraciones a la seguridad de los datos personales del H. Congreso del Estado, se debe generar la bitácora de vulneraciones, que deberá implementarse y conservarse en cada una de las áreas de este Honorable Congreso del Estado para el registro histórico y conocimiento de las vulneraciones que se presenten a lo largo del tiempo.

De conformidad con los medidas señaladas en el artículo 53 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados en el Estado de Chiapas señala, que la bitácora debe contener, cuando menos, fecha en que ocurrió el incidente, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva para evitar la continuidad de las vulneraciones.

El aviso de las vulneraciones ocurridas al titular de los datos personales, se realizará en los plazos que señala el artículo 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Chiapas, debiendo informarle lo siguiente:

1) La naturaleza del incidente
2) Los datos personales comprometidos
3) Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses
4) Las acciones correctivas realizadas de forma inmediata, y
5) Los medios donde puede obtener mayor información al respecto.

Ante la presencia de algún siniestro, con el propósito de asegurar un control adecuado en el momento que ocurre una vulneración y garantizar la no repetición de las mismas, lo conducente es implementar los mecanismos

señalados en la Fracción XV Gestión de Vulneraciones, del Documento de Seguridad del H. Congreso del Estado.

III. Designación de personas.

Es necesario designar a las personas que deberán intervenir en el momento que ocurra un siniestro, una vez que, cese el peligro o riesgo de la contingencia. El personal designado deberá llevar a cabo las tareas que sean idóneas para garantizar la seguridad y conservación de los datos personales.

En el supuesto de desastres de alto impacto (terremoto o incendio) donde implique perdidas estructurales, es necesario contar con un lugar alterno para llevar a cabo los trabajos que resulten necesarios y de atención inmediata.

IV. Investigación de la vulneración ocurrida.

Una vez ocurrida la vulneración ocurrida por un siniestro, de manera inmediata se debe iniciar una investigación, para determinar los alcances de los daños y la situación actual en que se encuentra la información que contiene datos personales.

Para ello, es importante involucrar al personal encargado de los procesos de tratamiento de los datos personales, y recabar toda la evidencia que sirva para documentar los daños ocurridos.

V. Medidas de prevención y conservación de archivos:

Los archivos que forman parte del acervo documental del H. Congreso del Estado, están expuestos a los riesgos producidos por calamidades y emergencias causadas por desastres naturales o por el hombre. En ese sentido, es de vital importancia contar con los mecanismos idóneos para la protección y conservación documental, este documento precisamente tiene como finalidad determinar las acciones de respuesta ante cualquier siniestro causado, particularmente los que se señalan en el rubro que continúa.

- El área del archivo general debe situarse en el primer piso del edificio (no sótanos)
- Espacios deben contar con luz natural y sin humedad.
- El mobiliario de archivos debe garantizar la conservación de los documentos que se resguardan; los documentos deben guardar uniformidad.
- Se debe evitar el archivo de documentos cerca de los aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas).
- Los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- No debe colocarse vasos o recipientes con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

VI. Medidas Preventivas ante Siniestros.

Previo a concretar las acciones a implementarse ante un siniestro, es muy importante planear como se debe preparar el H. Congreso del Estado de Chiapas para su eventual ocurrencia, en ese tenor es indispensable identificar lo siguiente:

- Recursos disponibles
- Identificar los documentos de archivo que contiene información de datos personales
- Designar al personal que brindará apoyo en las labores de recuperación y preparar los roles que deben asumir antes, durante y después del siniestro.
- Identificar equipos y materiales disponibles que sean necesarios al momento de atender la emergencia.

Enseguida se detallan las medidas que deberán implementarse en caso de ocurrir los siguientes siniestros:

- Incendio
- Terremoto o sismo
- Inundaciones por lluvia
- Robo
- Huelga o Manifestaciones
- Amenazas informáticas (hackeo informático)

A) Medidas preventivas para evitar un incendio.

- Se recomienda tener un conocimiento básico de primeros auxilios.
- Para la detección inmediata de un incendio es necesario contar con detectores de humo.

- Recibir capacitación para saber cómo actuar en caso de incendios.
- Evitar el almacenamiento sustancias inflamables, si fuera necesario se sugiere colocarlos en lugares ventilados y lejos de factores que propicien un incendio.
- No sobrecargar los contactos eléctricos, y se debe desconectar los que no se utilicen.

1.- Resguardo de Información en caso de Incendio.

- Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, en lugares cercanos a los extintores (sugerencias para almacenamiento: CD, Disco duro, base de datos, la nube únicamente si es segura)
- Tener identificados los documentos con mayor valor documental histórico para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube).
- El usuarios deberá realizar constantemente el respaldo y resguardo de la información
- El usuario de los procesos de alto riesgo es responsable de la información que resguarda en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.
- Realizar las acciones y mecanismos disponibles en materia de tecnología relacionados con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.
- Contar con expedientes electrónicos

2.- Durante un Incendio:

- Ubicar los extintores en lugares visibles y de fácil acceso y que éstos se encuentren en condiciones óptimas.
- El personal designado debe contar con conocimiento para usar un extintor.
- Integración de la Brigada contra Incendios
- Capacitación constante para el personal designado que permita la reacción inmediata ante un incendio.
- Debe mantenerse la calma y realizar el reporte de forma inmediata mediante los medios señalados para tal fin.
- Salir del inmueble inmediatamente.
- Si hay gas o humo lo recomendable es usar un trapo húmedo para cubrir la nariz y boca.
- En caso de incendio de baja intensidad, se procurará sofocarlo mediante el extintor

3.- Después del Incendio:

- Revisar el área o espacio donde se originó el incendio y evaluar daños
- Personal técnico debe revisar las instalaciones de gas y electricidad antes de ser utilizadas.
- Se debe contar con un reporte o dictamen emitido por personal de Protección Civil Municipal o Estatal, que sirva de sustento para evaluar los daños y condiciones para la normalización de actividades.
- Evaluación de daños y reporte de las vulneraciones acontecidas a través de las bitácoras correspondientes.

B) Medidas preventivas ante un Terremoto o Sismo:

Los daños ocasionados por un sismo o terremoto pueden ocasionar severos daños principalmente a la estructura del edificio que ocupa el recinto legislativo; en ese sentido, es prioridad el almacenamiento de los datos personales que se encuentran en dispositivos como Discos compactos o memorias extraíbles, lo recomendable es contar con un respaldo de información en la nube, donde se mantendrá a salvo de cualquier eventualidad que signifique su pérdida o daño.

- Evitar colocar objetos o mobiliario que bloqueen las rutas y salidas de emergencia.
- Implementar líneas telefónicas de emergencia en caso no sea posible utilizar las líneas telefónicas fijas.
- Realizar simulacros con frecuencia y establecer mecanismos de evacuación.
- Identificar lugares seguros, como muros, mesas sólidas y escritorios resistentes, que permitan protegerse.
- Colocar señalamientos que indiquen la ruta de evacuación
- Integración de la Brigada de Sismo o Terremoto.

1.- Resguardo de Información en caso de sismo o terremoto.

- El usuarios deberá realizar constantemente el respaldo y resguardo de la información
- El usuario de los procesos de alto riesgo es responsable de la información que resguarda en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.

- Realizar las acciones y mecanismos disponibles en materia de tecnología relacionados con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.
- Contar con expedientes electrónicos.

2.- Durante un Sismo o terremoto.

- Mantener la calma no correr o empujar, salir del edificio de forma ordenada.
- Ubicarse en la zona segura, previamente señalada.
- Pararse bajo una puerta de marco con trabe o de espaldas a un muro de carga, en caso no sea posible la evacuación inmediata.
- Alejarse de ventanas y puertas de cristal que pudieran estrellarse, así como techos u objetos colgantes que pudieran caerse causando daños en la integridad física de las personas.
- No permanecer cerca de libreros, gabinetes o muebles pesados que al momento del siniestro, suelen caer y causar daño.
- Evitar el uso de elevadores en edificios y utilizar escaleras.
- Si es posible desconectar la alimentación eléctrica.

3.- Después del sismo o terremoto:

- Revisión y evaluación de daños
- Personal Técnico debe revisar las instalaciones de gas y electricidad antes de ser utilizadas.

- Se debe contar con un reporte o dictamen emitido por personal de Protección Civil Municipal o Estatal, que sirva de sustento para evaluar los daños y condiciones para la normalización de actividades.
- Evaluación de daños y reporte de las vulneraciones acontecidas a través de las bitácoras correspondientes.

C) Medidas de Prevención en caso de Inundación:

Las inundaciones causadas por lluvia pueden ocasionar daños considerables en edificaciones o lugares vulnerables ante este fenómeno natural. Cuando se produce una inundación, bien sea de pocos centímetros o hasta de metros de altura en casos muy extremos, el material u objetos que estén sobre el piso van a absorber gran parte del agua que entre en contacto con ellos. De igual modo, el ambiente del lugar también va absorber vapor de agua y por consiguiente se elevarán los niveles de humedad.

De manera enunciativa más no limitativa se enuncian las siguientes recomendaciones:

- Realizar labores de mantenimiento y reparación de la hermeticidad de ventanas y puertas del edificio, donde podría filtrarse el agua de la lluvia, así como impermeabilizar los techos en temporada de lluvias para evitar goteras o filtraciones de agua.
- No colocar expedientes y/o documentos directamente en el piso.
- Proteger el cableado eléctrico

1.- Resguardo de Información en caso de Inundación:

- No colocar expedientes y/o documentos directamente en el piso.
- El usuarios deberá realizar constantemente el respaldo y resguardo de la información
- El usuario de los procesos de alto riesgo es responsable de la información que resguarda en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.
- Realizar las acciones y mecanismos disponibles en materia de tecnología relacionados con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.
- Contar con expedientes electrónicos.

2.- Durante una inundación:

Desconectar servicios de luz eléctrica.

- No tocar ni pisar cables eléctricos.
- Evacuar el área si es necesario.

3.- Después de la inundación:

- Evaluar los daños causados y emitir el reporte correspondiente
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de las inundaciones.
- Identificar la documentación dañada e iniciar su proceso de restauración en lo posible

D) Medidas de prevención en caso de Robo.

Ante el robo común de equipos se deben tomas las siguientes medidas para el resguardo de información que contiene datos personales:

- El usuarios deberá realizar constantemente el respaldo y resguardo de la información
- El usuario de los procesos de alto riesgo es responsable de la información que resguarda en la carpeta asignada por la Unidad de Informática, para realizar el respaldo de manera periódica.
- Realizar las acciones y mecanismos disponibles en materia de tecnología relacionados con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.
- Contar con expedientes electrónicos.

E) Medidas de Prevención en caso de Huelgas y/o Manifestaciones:

- Asegurarse de cerrar con llave las puertas de oficinas
- Asegurase que archiveros o muebles que contengan información queden bajo llave.
- Resguardo de documentos e información en lugares seguros, archiveros, cajones, gavetas, puertas de oficinas con cerraduras y llaves

1.- Después de la manifestación o huelga:

- Evaluación de posibles daños a la información resguardada
- Emitir el reporte correspondiente en caso de alguna vulneración

E) Medidas Preventivas por Amenazas Informáticas (Hackeo informático):

Es el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

- Para prevención de fallas de los equipos: se debe pedir al área de Informática de este Honorable Congreso del Estado para que de mantenimiento preventivo por lo menos dos veces al año.
- Contar con reguladores en cada uno de los equipos, para evitar daños en los equipos por fallas eléctricas.
- Actualizaciones del sistema operativo, antivirus actualizados y copias de respaldo.
- Hacer implementación y uso del servidor.
- Cambio de claves de acceso mínimo cada seis meses. Implementado la política de seguridad para acceso de personal competente.
- Realizar una copia de seguridad en algún medio de almacenamiento (discos compactos, USB, entre otros) de todos los sistemas del H. Congreso del Estado y archivos del PC al menos para ser realizados cada viernes al término de la jornada.

Ante la sospecha de un evento de hackeo informático es necesario informar al área de informática de este Honorable Congreso del Estado para que le den seguimiento y realicen las acciones pertinentes para el respaldo y cuidado de los datos personales.

De conformidad con el artículo 113 y 114, fracciones I, VI y VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas, con fecha veintiséis de septiembre del dos mil veintitrés, el Comité de Transparencia aprueba el Plan de Contingencias en materia de Protección de Datos Personales del H. Congreso del Estado.