**GUIA PARA EL TRATAMIENTO DE DATOS PERSONALES**

**SALA DE DIPUTADOS Y DIPUTADOS DEL CONGRESO**

**DEL ESTADO DE JALISCO.**

**LXII LEGISLATURA**

**CONTENIDO GENERAL**

Glosario…………………………………………………..…………………………………………….…... 3

Introducción……………………………………………………………………………………………….. 7

Aplicación de la ley de protección de datos personales en posesión

de sujetos obligados del Estado de Jalisco y sus Municipios……………….………………………. 7

Principios rectores de los datos personales……………………………………..………..…………… 8

Principio de licitud ………………………………………………………………………………...……… 9

Principio de finalidad ……………………………………………………………...…………………..…. 12

Principio de proporcionalidad ……………………………………………………….……………..…… 13

Principio de información …………………………………………………………………………………. 14

Principio de consentimiento ………………………………………………………………………..…… 22

Principio de lealtad ……………………………………………………………………..…………….…. 23

Principio de calidad ……………………………………………………………………..……………… 23

Principio de responsabilidad …………………………………………………………………………... 25

Objetivo del Documento de seguridad …………………………………………….........………...…. 27

¿Qué es el Documento de seguridad? ………………………………………………………..…..… 27

Medidas de seguridad ……………………………………………………………..……………..…..… 27

Contenido del documento de seguridad ……………………………………………………………… 30

Documento de Seguridad “Sala de Diputados”…………………………….……………………...…. 33

Anexos………….…………………………………………………………………………………………. 60

Avisos de privacidad…………………….………………………..……………………………………… 71

**GLOSARIO**

**Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

**Aviso de privacidad**: Documento físico, electrónico o en cualquier formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales.

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

**Bloqueo:** La identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual correspondiente. Durante dicho periodo los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda.

**Comité de Transparencia:** Es el órgano interno del sujeto obligado encargado de la clasificación de la información pública. Su integración es la siguiente:

I.- El titular del sujeto obligado cuando sea unipersonal o el representante oficial del mismo cuando sea un órgano colegiado, quien lo presidirá;

II.- El titular de la Unidad de Transparencia, quien fungirá como Secretario.

III.- El titular del órgano con funciones de control interno del sujeto obligado cuando sea unipersonal o el representante oficial del mismo cuando sea un órgano colegiado.

**Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos digitales, en recursos compartidos dinámicamente.

**Consentimiento:** Manifestación de la voluntad libre, especifica e informada del titular que autoriza el tratamiento de sus datos personales.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa e indirectamente a través de cualquier información.

**Datos personales sensibles:** Aquellos que se refieren 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 pueden revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, 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.

**Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

**Documento de seguridad:** 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.

**Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.

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

**Ley:** Ley de protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios.

**Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**Medidas compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

**Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

**Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales.

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

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

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

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

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

**Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

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

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

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

**Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano.

**Responsable:** Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medio y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

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

**Titular:** Persona física a quien pertenecen los datos personales.

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

**Tratamiento:** De manera enunciativa más no limitativa 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; y

**Unidad de Transparencia:** Instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

**INTRODUCCIÓN.**

El objetivo de esta Guía de Tratamiento, es acompañar a los responsables de este sujeto obligado para la protección de datos personales ya que es un derecho que permite a las personas controlar la información que comparten con otros, así como el derecho para que dicha información sea usada de forma adecuada para permitir el ejercicio de otros derechos y evitar daños a su intimidad y privacidad; así como el cumplimiento de las obligaciones señaladas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

**APLICACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS**

Esta Ley tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

Son sujetos obligados por esta Ley, en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo del Poder Ejecutivo y Judicial, ayuntamientos, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que lleven a cabo el tratamiento de datos personales.

Los sindicatos y cualquier otra persona física o jurídica que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares, sin perjuicio de lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios es aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia del lugar, la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**PRINCIPIOS RECTORES DE LOS DATOS PERSONALES**

Con la protección de datos el derecho que se trata de proteger no es solamente el de la intimidad, sino el de la Privacidad, la protección se realizara sobre el dato, de manera que éste no pueda ser tratado o elaborado y convertido en información nada más para aquellos fines y por aquellas personas autorizadas.

 No se puede tratar ningún dato de carácter personal sin el consentimiento del titular o del interesado, salvo que concurra en alguna excepción prevista en el Titulo Quinto “Comunicaciones de datos personales” de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; Los datos Personales se deben tratar en la forma especificada en los principios de protección de datos y facilitar el ejerció de los derechos de los ciudadanos.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece y reconoce los principios, deberes y derechos rectores de la protección de datos personales y que en su conjunto garantizan un adecuado manejo de los mismos.

De acuerdo con el artículo 9 de La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios los principios rectores de la protección de los Datos Personales son:

**1.- PRINCIPIO DE LICITUD**

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

*Articulo 10. Principio de Licitud.*

*1.- Sera licito el tratamiento de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable les confiera y deberán obtenerse a través de los medios previstos en dichas disposiciones.*

\* Debemos de conocer la normatividad, ya que en lo especifico regula el derecho a la protección de datos personales y se debe realizar el tratamiento en plena observancia de la misma.

Los Datos Personales que se recaban (inventario) en el área de la Unidad de Transparencia del Congreso del Estado son los siguientes:

*DATOS DE IDENTIFICACIÓN:*

* *Nombre completo.*
* *Fecha de nacimiento.*
* *Lugar de nacimiento.*
* *Nacionalidad.*
* *Estado civil.*
* *Domicilio particular.*
* *Número de teléfono.*
* *Correo electrónico.*
* *Identificación oficial.*
* *Copia de identificación oficial.*
* *Carta de no antecedentes penales.*
* *Constancia de no sanción administrativa.*

 *DATOS FISCALES:*

* *Clave Única de Registro de Población (CURP).*
* *Registro Federal de Contribuyentes (RFC).*
* *Razón social.*
* *Marca comercial.*
* *Giro comercial (personas físicas).*
* *Domicilio fiscal.*
* *Acta Constitutiva con sus modificaciones.*
* *Poder del Representante Legal.*
* *Número de registro patronal.*
* *Constancia de situación fiscal expedida por la Secretaría de Hacienda y Crédito Público.*

*DATOS PATRIMONIALES:*

* *Datos bancarios.*
* *Datos de créditos.*
* *Datos de catastro.*
* *Bienes muebles.*
* *Bienes inmuebles.*

*DATOS DE TERCEROS:*

* *Nombre de los beneficiarios.*
* *Parentesco, números telefónicos y referencias en caso de accidente.*

*DATOS ACADÉMICOS:*

* *Título o cédula profesional.*
* *Comprobante de estudios del último nivel alcanzado.*
* *Conocimiento en idiomas (documento probatorio).*

*DATOS LABORALES:*

* *Datos de empleos anteriores*
* *Cargo.*
* *Puesto.*

*DATOS PERSONALES SENSIBLES:*

* *Firma.*
* *Fotografía.*
* *Sexo.*
* *Rasgos físicos.*
* *Imagen en la grabación.*
* *Discapacidad.*

*\* Datos biométricos:*

* *Huella dactilar.*
* *Reconocimiento facial.*
* *Tipo de sangre.*

*\* Datos de salud:*

* *Certificado médico.*

**2.- PRINCIPIO DE FINALIDAD**

*Articulo 11.- principio de Finalidad.*

*1.- Todo tratamiento de datos personales que efectúe el responsable deberá ser justificado por finalidades concretas, explicitas, licitas y legítimas y deberá sujetarse a los principios contenidos en el presente capitulo, relacionadas con las facultades y atribuciones que la normatividad aplicable les confiera.*

*2. Se entenderá que las finalidades son:*

*I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan generar confusión en el titular;*

 *II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad; y*

*III. Lícitas y legítimas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional aplicable.*

*3. El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en esta Ley y demás disposiciones aplicables.*

\* Los datos personales solo deben ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al Titular en el aviso de privacidad. Se entiende por finalidad del tratamiento, el motivo, propósito o razón por el cual se trata los datos personales; las cuales deben ser determinadas, deberá especificar para que objeto se trataran los datos personales de manera clara, sin confusión y con objetividad.

**3.- PRINCIPIO DE PROPORCIONALIDAD**

*Artículo 18. Principios — Criterio de minimización. 1. El responsable procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.*

\* Solo podrán ser objeto de tratamiento los datos personales que sean necesarios, adecuados y relevantes en relación con las finalidades para lo que se haya obtenido y se encuentren previstas en el aviso de privacidad.

**4.- PRINCIPIO DE INFORMACIÓN**

*Artículo 19. Principios — Información.*

*1. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.*

 *2. El aviso de privacidad tendrá por objeto informar al titular sobre los alcances y condiciones generales del tratamiento, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales y, en consecuencia, mantener el control y disposición sobre ellos.*

*3. El aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que se cuente, tales como medios impresos, sonoros, digitales, visuales o cualquier otra tecnología; con una redacción y estructura clara y sencilla, para cumplir con el propósito de informar.*

 *4. Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.*

 *5. El aviso de privacidad se redactará conforme a lo dispuesto en la Ley General.*

 *6. En el caso de personas indígenas, el responsable hará los ajustes razonables pertinentes para dar a conocer el aviso de privacidad en su lengua de origen, con el objetivo de que el consentimiento sea considerado libre. Lo mismo aplicará para personas que comprendan el sistema braille y análogos.*

\* En este principio el Responsable está obligado a elaborar y poner a disposición el Aviso de Privacidad, ya que debe comunicar al Titular de los datos personales las características principales del tratamiento al que será sometida su información personal, así como los medios para ejercer sus derechos, lo que se materializa a través del Aviso de Privacidad.

***AVISO DE PRIVACIDAD INTEGRAL***

***CONGRESO DEL ESTADO DE JALISCO***

***RESPONSABLE DEL TRATAMIENTO***

*El Congreso del Estado de Jalisco, con domicilio en Avenida Hidalgo número 222, colonia Centro en Guadalajara, Jalisco, Código Postal 44100, es el responsable del tratamiento de los datos personales proporcionados, los cuales serán protegidos conforme a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, y demás normatividad; al respecto le informa lo siguiente:*

*Los datos personales se refieren a la información concerniente a una persona física identificada o identificable, siendo los datos personales sensibles aquellos que afecten a la esfera más íntima de su titular o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.*

***ATRIBUCIONES LEGALES PARA EL TRATAMIENTO DE LOS DATOS PERSONALES***

*El tratamiento de sus datos personales se realiza con fundamento en lo establecido en:*

* *La Constitución Política de los Estados Unidos Mexicanos: Artículos 6 apartado A fracciones II y VI y 16 párrafo segundo.*
* *La Constitución Política del Estado de Jalisco: Artículos 4 párrafo séptimo y 9 fracciones II, V y VI.*
* *La Ley General de Transparencia y Acceso a la Información Pública: Artículos 23; 49; 50 y 68.*
* *La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios: Artículos 20 y 66.*
* *La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: Artículos 1 párrafo cuarto; 3 fracciones II, IX, X, XXVII; 26; 27 y 28.*
* *La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios: Artículos 1 párrafo segundo y tercero; 3 fracciones III, IX, X, XI y XXXII; 10; 11; 21; 87 fracción I y 88 fracción I.*
* *La Ley Orgánica del Poder Legislativo del Estado de Jalisco: Artículos 1 y 2.*

***¿QUE DATOS PERSONALES SE RECABAN?***

*Los datos personales que serán sometidos a tratamiento son:*

*DATOS DE IDENTIFICACIÓN:*

* *Nombre completo.*
* *Fecha de nacimiento.*
* *Lugar de nacimiento.*
* *Nacionalidad.*
* *Estado civil.*
* *Domicilio particular.*
* *Número de teléfono.*
* *Correo electrónico.*
* *Identificación oficial.*
* *Copia de identificación oficial.*
* *Carta de no antecedentes penales.*
* *Constancia de no sanción administrativa.*

 *DATOS FISCALES:*

* *Clave Única de Registro de Población (CURP).*
* *Registro Federal de Contribuyentes (RFC).*
* *Razón social.*
* *Marca comercial.*
* *Giro comercial (personas físicas).*
* *Domicilio fiscal.*
* *Acta Constitutiva con sus modificaciones.*
* *Poder del Representante Legal.*
* *Número de registro patronal.*
* *Constancia de situación fiscal expedida por la Secretaría de Hacienda y Crédito Público.*

*DATOS PATRIMONIALES:*

* *Datos bancarios.*
* *Datos de créditos.*
* *Datos de catastro.*
* *Bienes muebles.*
* *Bienes inmuebles.*

*DATOS DE TERCEROS:*

* *Nombre de los beneficiarios.*
* *Parentesco, números telefónicos y referencias en caso de accidente.*

*DATOS ACADÉMICOS:*

* *Título o cédula profesional.*
* *Comprobante de estudios del último nivel alcanzado.*
* *Conocimiento en idiomas (documento probatorio).*

*DATOS LABORALES:*

* *Datos de empleos anteriores*
* *Cargo.*
* *Puesto.*

*DATOS PERSONALES SENSIBLES:*

* *Firma.*
* *Fotografía.*
* *Sexo.*
* *Rasgos físicos.*
* *Imagen en la grabación.*
* *Discapacidad.*

*\* Datos biométricos:*

* *Huella dactilar.*
* *Reconocimiento facial.*
* *Tipo de sangre.*

*\* Datos de salud:*

* *Certificado médico.*

*Dichos datos podrán ser recabados, directa o indirectamente, por medios electrónicos, por escrito y vía telefónica, los datos personales que usted proporcione al Congreso del Estado de Jalisco, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Congreso.*

***FINALIDADES DEL TRATAMIENTO***

*Los datos personales serán utilizados para las siguientes finalidades:*

* *Dar cumplimiento con la obligación de la presentación de las declaraciones de situación patrimonial de Interés y constancia de declaración fiscal.*
* *Integrar el expediente de registro y control de la situación patrimonial del Servidor Público.*
* *Verificar la evolución y congruencia entre los ingresos y egresos del Servidor Público.*
* *Conocer los posibles conflictos de intereses del Servidor Público.*
* *Investigar y calificar presuntas faltas administrativas e imponer sanciones a los servidores públicos o particulares según corresponda.*
* *Investigar, substanciar y resolver los expedientes, relativos a procedimientos de responsabilidad administrativa que conoce el Órgano Interno de Control del Congreso del Estado de Jalisco.*
* *Llevar los registros de los asuntos y expedir las certificaciones de los documentos que se encuentren en el Órgano Interno de Control del Congreso del Estado de Jalisco.*
* *Citar, iniciar e instruir el procedimiento de responsabilidad administrativa así como sancionar.*
* *Garantizar la entrega-recepción de todos los recursos materiales, humanos, patrimoniales, financieros y documental que hayan estado a la disposición del Servidor Público.*
* *Verificar, comprobar y dar certeza de todo aquello que estuvo bajo la responsabilidad del Servidor Público dentro del espacio físico que ocupaba en el Congreso del Estado de Jalisco, sea entregado al concluir el empleo, cargo o comisión.*
* *Realizar actas de entrega-recepción.*
* *Instaurar el procedimiento de determinación de responsabilidad administrativa.*
* *Obtener y resguardar los Datos Personales de los interesados en realizar denuncias en contra de los Servidores Públicos del Congreso de Estado de Jalisco.*
* *Notificar como tercer interesado de la realización de la denuncia en contra de los Servidores Públicos del Congreso de Estado de Jalisco.*
* *Mantener el control de entradas de quien ingresan al Congreso del Estado de Jalisco.*
* *Verificar y confirmar su identidad, Integrar expedientes con solicitudes de Derecho ARCO.*
* *Integrar expedientes relativos a solicitudes de acceso a la información.*
* *Entregar la información solicitada vía presencial, vía infomex, vía correo electrónico, vía comparecencia.*
* *Entregar información solicitada por cualquier otro medio de los autorizados en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.*
* *Recabar los datos personales requeridos para la integración y control de los expedientes de los prestadores de servicio social y prácticas profesionales a fin de emitir la respectiva carta de terminación.*
* *Elección o ratificación de servidores públicos de la competencia del Congreso.*
* *Procedimientos de responsabilidad política.*
* *Dar cumplimiento a las obligaciones y trámites tributarios, legales y administrativas inherentes a este congreso.*
* *Sustanciación del trámite para la designación de Ayuntamientos y suspensión o revocación de mandato a algunos de sus miembros.*
* *El registro de los participantes, ponentes e invitados a los eventos, capacitaciones y convocatorias que promueve el Congreso del Estado de Jalisco.*
* *Procesos en los que se analizan los informes finales de las cuentas públicas y estados financieros derivados del proceso de fiscalización.*

*Se utilizan cookies al momento en que usted navega en el sitio oficial del Congreso del Estado de Jalisco:* [*www.congresojal.gob.mx*](http://www.congresojal.gob.mx) *mismos que usted puede administrar o bloquear desde su navegador de internet.*

***TRANSFERENCIA DE DATOS PERSONALES***

*Se informa que no realizarán transferencias que requieran su consentimiento, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente, debidamente fundados y motivados. Conforme a lo dispuesto en los artículos 70; 71; 72; 73; 74 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.*

***¿DONDE SE PUEDE EJERCER LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN AL TRATAMIENTO DE DATOS PERSONALES?***

*Tiene el derecho a conocer qué datos personales se tienen de usted, para qué se utilizan y las condiciones del uso que les damos (Acceso); asimismo, es su derecho solicitar la corrección de su información personal en caso de que este desactualizada, sea inexacta o incompleta (Rectificación); que la eliminemos de nuestros registros de bases de datos cuando considere que la misma no está siendo utilizada conforme a los principios, deberes y obligaciones previstas en la ley (Cancelación); así como oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO; conforme a lo establecido en el artículo 45 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.*

*Para el ejercicio de los derechos ARCO, usted podrá presentar solicitud ante la Unidad de Transparencia por escrito; en formato electrónico, a través de la Plataforma Nacional de Transparencia disponible en:* [*https://www.plataformadetransparencia.org.mx/web/guest/inicio*](https://www.plataformadetransparencia.org.mx/web/guest/inicio)*; el sistema infomex Jalisco:* [*www.infomexjalisco.org.mx*](http://www.infomexjalisco.org.mx) *y finalmente por correo electrónico en la dirección:* *transparencia@congresojal.gob.mx**.*

***DIRECCIÓN DE LA UNIDAD DE TRANSPARENCIA:***

*Av. Juárez 237, Primer Piso, Colonia Centro, Guadalajara, Jalisco.*

*Teléfono: 33 36 79 15 00.*

 *Ext: 4060.*

***CONSENTIMIENTO Y CAMBIOS AL AVISO DE PRIVACIDAD***

*Por así convenir a mi interés jurídico, entiendo y otorgo mi consentimiento para que mis datos personales sean tratados conforme a lo enunciado en el presente Aviso de Privacidad, quedando plenamente enterado de su manejo y tratamiento por el* ***CONGRESO DEL ESTADO DE JALISCO.*** *Así mismo entiendo y otorgo mi consentimiento, para la transmisión de datos que proporcioné para los fines enunciados en el aviso de privacidad.*

*En caso de realizar alguna modificación al aviso de privacidad se le hará de su conocimiento a través de la página de internet de este sujeto obligado: www.congresojal.gob.mx.*

***AVISO DE PRIVACIDAD SIMPLIFICADO.***

***CONGRESO DEL ESTADO DE JALISCO***

*El Congreso del Estado de Jalisco, con domicilio en Avenida Hidalgo # 222, colonia Centro en Guadalajara, Jalisco, Código Postal 44100, es el responsable del tratamiento de los datos personales proporcionados, los cuales serán protegidos conforme a lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, y demás normatividad aplicable. Sus datos personales serán utilizados para las siguientes finalidades: A) Dar cumplimiento a las obligaciones y trámites legales y administrativos inherentes a este Congreso. Así como los demás objetivos y atribuciones de este Poder Legislativos, establecidos en el aviso de privacidad integral.*

*Se informa que no se realizarán transferencias sin su consentimiento, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente, debidamente fundados y motivados. Conforme a lo dispuesto en los artículos 70,71, 72, 73, 74, 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Si desea conocer nuestro aviso de privacidad integral lo podrá consultar a través de la página de internet de este sujeto obligado la cual es:* [*www.congresojal.gob.mx*](http://www.congresojal.gob.mx) *en la sección de “Avisos de Privacidad” o de manera presencial en nuestras instalaciones.*

***AVISO DE PRIVACIDAD CORTO***

***SALA DE DIPUTADOS Y DIPUTADAS***

*Por este medio se le informa que en términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; El Congreso del Estado de Jalisco, con domicilio en Avenida Hidalgo # 222, colonia Centro en Guadalajara, Jalisco, Código Postal 44100, es el responsable del uso y protección de los datos personales, y al respecto le informa lo siguiente: Los Datos Personales que proporcione es información confidencial y serán utilizados para los fines establecidos.*

*Usted puede consultar nuestro Aviso de Privacidad integral a través de la página de internet de este sujeto obligado, la cual es:* [*www.congresojal.gob.mx*](http://www.congresojal.gob.mx)*, en la sección de “avisos de privacidad” o bien de manera presencial en nuestras instalaciones.*

**5.- PRINCIPIO DE CONSENTIMIENTO**

*Artículo 14. Principios — Tipos de Consentimiento.*

*1. El consentimiento podrá manifestarse de forma expresa o tácita. El consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. En el entorno digital, podrá utilizarse la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular y, a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo.*

 *2. Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad.*

 *3. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando el aviso de privacidad es puesto a disposición y éste no manifiesta su voluntad en sentido contrario.*

 *4. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en esta Ley.*

Estos dos principios con el Aviso de Privacidad se cumplen, al ponerlo en zonas de fácil acceso, a la vista o que se ponga a disposición de forma directa a los titulares, previa la entrega de sus datos personales, y se entenderá que el consentimiento es tácito, siempre y cuando el titular no manifieste lo contrario después de conocer el aviso.

**6.- PRINCIPIO DE LEALTAD**

*Artículo 12. Principios — Lealtad.*

*1. El responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos; deberá privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad.*

 *2. Se estará en presencia de un tratamiento engañoso o fraudulento cuando:*

*I. Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo;*

 *II. Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular, o*

*III. Vulnere la expectativa razonable de protección de datos personales.*

**7.- PRINCIPIO DE CALIDAD**

***Artículo 16.*** *Principios — Calidad.*

*1. El principio de calidad de los datos personales requiere que el responsable adopte medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.*

*2. Se presume que se cumple con el principio de calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.*

*3. Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, deberán ser suprimidos, previo bloqueo en su caso y una vez que concluya el plazo de conservación de los mismos.*

Los datos personales deberán ser CONSERVADOS, BLOQUEADOS Y SUPRIMIDOS, atendiendo al ciclo de la vida de los datos personales.

Los datos personales no se deben tratar indefinidamente, solo por el periodo de tiempo necesario para cumplir las finalidades por las que fueron recolectados.

Para este procedimiento, la Ley General de Archivos contempla un capítulo

 (Articulo 60 al 63), en cuanto a la conservación de los archivos.

**TECNICAS DE SUPRESIÓN Y BORRADO:**

***Desmagnetización:***

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos como por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético del que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

***Destrucción física:***

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades especificas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: Las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos.

Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

***Sobre-escritura:***

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no sean regrabables, como los CD y DVD.

**8.- PRINCIPIO DE RESPONSABILIDAD**

*Artículo 28. Principios — Responsabilidad.*

*1.- El responsable deberá implementar los mecanismos necesarios para cumplir con los principios, deberes y obligaciones establecidos en esta Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular o al Instituto, según corresponda; observando la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.*

**CONGRESO DEL ESTADO DE JALISCO**

**DOCUMENTO DE SEGURIDAD**

**“SALA DE DIPUTADOS Y DIPUTADAS”**

**1.- OBJETIVO DEL DOCUMENTO**

Identificar los principales elementos en materia de protección de datos personales relacionados con las medidas de seguridad físicas, digitales, administrativas y técnicas, a fin de determinar y difundir las vulnerabilidades, amenazas y riesgos.

El Congreso del Estado de Jalisco mantiene un tratamiento de datos personales para los cuales realiza la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición o cualquier otra operación aplicable a ellos.

**2.- DOCUMENTO DE SEGURIDAD.**

Con el presente “Documento de Seguridad” se cumple con las disposiciones del capítulo II “Deberes” de los artículos 30 al 44 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Como Documento de Seguridad se entiende: Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que deberán estar documentadas y contenidas en un sistema de gestión.

El Documento de Seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

Por Sistema de Gestión se entiende: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

**3.- MEDIDAS DE SEGURIDAD.**

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Existen diferencias entre las medidas de seguridad:

*A).- Las medidas de Seguridad Administrativas:* Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales.

*B) Las medidas de Seguridad Físicas:* Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento; se consideran las siguientes actividades:

\* Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

\* Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.

\* Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y

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

*C) Las Medidas de Seguridad Técnicas:* Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento; se consideran las siguientes actividades:

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

\* Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

\* Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

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

Existen dos tipos de Soportes: Físicos y Electrónicos.

\* Soportes Físicos: Son los medios de almacenamiento intangibles a simple vista, es decir que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otro.

\* Soporte Electrónicos: Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir cintas magnéticas de audio, video y datos, fichas de microfilm, discos ópticos ( CDs y DVDs), discos magneto-ópticos, discos magnéticos ( flexibles y duros) y demás medios de almacenamiento masivo no volátil. El documento de seguridad deberá constar si los datos personales del sistema residen en:

I) Soporte físicos.

II) Soporte electrónico.

III) Ambos tipos de soportes.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar las siguientes acciones:

\* Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

\* Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

\* Elaborar un inventario de datos personales y de los sistemas de tratamiento.

\* Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

\* Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

\* Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

\* Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

**4.- CONTENIDO DEL DOCUMENTO DE SEGURIDAD.**

El documento de seguridad deberá contener:

1.- El nombre de los sistemas de tratamiento o base de datos personales.

2.- El nombre, cargo y adscripción del administrador de cada sistema de tratamiento y/o base de datos personales.

3.- Las funciones y obligaciones de las personas que traten datos personales.

4.- El inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales.

5.- La estructura y descripción de los sistemas de tratamiento y/o base de datos personales señalando el tipo de soporte y las características del lugar donde se resguardan.

6.- *Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen:* Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

7.- *El resguardo de los soportes físicos y/o electrónicos de los datos personales*.

8.- *Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales:* Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos o electrónicos, y contienen la siguiente información:

|  |  |
| --- | --- |
| **BITÁCORA DE ACCESO** | \* Nombre y cargo de quien accede.\* Identificación del Expediente.\* Fojas del Expediente.\* Propósito del Acceso.\* Hora del acceso.\* Fecha del acceso.\* Fecha de Devolución.\* Hora de Devolución. |

|  |  |
| --- | --- |
| **VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES** | \* Nombre de quien reporta el incidente.\* Cargo.\* La fecha en la que ocurrió.\* El motivo de la vulneración de seguridad.\* Las acciones correctivas implementadas de forma inmediata y definitiva. |

9.- *El análisis de riesgos:* considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

10.- *El análisis de brecha:* Se realiza un diagnóstico de las prácticas de seguridad de la información con las que cuentan en ese momento al sujeto obligado y las que deberían de tenerse en base a las mejores prácticas.

11.- *La gestión de vulneraciones:* Una vulnerabilidad se considera una debilidad en la seguridad de los datos personales; aunque en sí misma no causa daño, puede afectar a algún dato cuando se aprovecha o explota por alguna amenaza.

|  |
| --- |
| **TIPO DE AMENAZAS** |
| **TIPO** | **EJEMPLO** |
| INTENCIONALES | 1. Accesos no autorizados a información o instalaciones.
2. Ataque malicioso (físico o lógico).
3. Personal interno mal intencionado.
4. Personas externas mal intencionado.
5. Explotación de vulnerabilidades tecnológicas.
 |
| NO INTENCIONALES | 1. Desastre natural.
2. Falla en el suministro de energía.
3. Error, accidente o descuido del personal.
4. Falla o descompostura en la infraestructura.
5. Demanda excesiva de servicios.
 |

12.- Las medidas de seguridad físicas aplicadas a las instalaciones.

13.- *Los controles de identificación y autenticación de usuarios:* Se debe señalar y detallar la forma en que se identifica el personal del sujeto obligado, así como la forma en que se autentifica a cada uno.

14.- *Los procedimientos de respaldo y recuperación de los datos personales:* Es el procedimiento que se implementa cuando queremos tener resguardados nuestros datos o documentos en caso de que suceda algún imprevisto con el sistema informático. Un respaldo de información bien organizado y estructurado nos permitirá volver a acceder a los documentos para continuar trabajando, y evitar que información importante se pierda.

15.- *El plan de contingencia:* Elaborar un plan de contingencia respecto a la seguridad y protección de los datos personales, en caso de vulneraciones.

16.- Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.

17.- *El plan de trabajo:* Para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

18.- Los mecanismos de monitoreo y revisión de las medidas de seguridad.

19.- *El programa general de capacitación:* Establecer un programa para capacitar al personal del sujeto obligado sobre el tema de protección de datos personales. Indicar la temporalidad de la capacitación, las áreas a capacitar, las sesiones y los temas.

|  |
| --- |
| FORMATO DOCUMENTO DE SEGURIDADPROTECCIÒN DE DATOS PERSONALES |
| I.- Nombre del Sistema o base de datos ( Área del Congreso del Estado de Jalisco)DIPUTADOS Y DIPUTADAS |
| II.- Administrador Responsable |
| Nombre: |  |
| Cargo: |  |
| Adscripción: |  |
| III.- Funciones y obligaciones del Responsable de los Datos Personales |
| 1.- Desempeñar al cargo con apego a las Constituciones federal y estatal, la Ley Orgánica del Poder Legislativo del Estado de Jalisco y su Reglamento y demás disposiciones aplicables, así como participar en todas las actividades inherentes al mismo.2.- Asistir a todas las sesiones que celebre el Congreso del Estado, en caso de falta injustificada se le reduce de su dieta, lo equivalente a un día de trabajo.3.- Asistir a las reuniones de comisión o comité, de los que formen parte, así como participar en las votaciones.4.- Acatar las disposiciones y encomiendas de la Asamblea y de la Presidencia de la Mesas Directiva que estén conformes con la Ley Orgánica del Poder Legislativo del Estado de Jalisco y su Reglamento.5.- Permanecer en el Recinto Oficial durante las sesiones de la Asamblea y las reuniones de las comisiones y comités convocados conforme al reglamento. Queda prohibido a los diputados y las diputadas abandonar el Recinto Oficial sin la autorización previa de la presidencia de la Mesa Directiva; en caso de hacerlo se tiene como inasistencia.6.- Informar permanentemente a la sociedad de sus actividades.7.- Abstenerse de realizar actos incompatibles con las funciones que desempeñan, así como de hacer valer su condición de legisladores en beneficio propio.8.- Abstenerse de desempeñar otro empleo, cargo o comisión de la Federación, del Estado, de los municipios o sus entidades, cuando se perciba sueldo, con excepción de las labores de docencia, investigación científica y beneficencia.9.- Abstenerse de intervenir en los asuntos legislativos, en los que tenga un interés personal, o que interesen a su cónyuge, concubina o concubinario, o a sus parientes consanguíneos en línea recta sin limitación de grados, o los colaterales dentro del cuarto grado y a los afines dentro del segundo, siempre que no se trate de disposiciones de carácter general.10.- Presentar en tiempo y forma las declaraciones de situación patrimonial , conflicto de interés y fiscal, e informes que establecen las normas aplicables o que estén obligados a rendir con motivo del desempeño de sus funciones o encomiendas conforme a las disposiciones legales aplicables.11.- Presentar iniciativas de ley, decreto o acuerdo legislativo dentro del tiempo que dure su encargo.12.- Percibir exclusivamente la remuneración establecida en el Presupuesto de Egresos del Poder Legislativo y de conformidad con la ley, sin que bajo ninguna circunstancia puedan recibir ingresos extraordinarios o por el fin del encargo, adicionales a la remuneración.13.- Las demás que señalen la Constitución, las leyes y disposiciones reglamentarias aplicables. |
| IV.- Inventario de los Datos Personales |
| ORDINARIOS: |  SENSIBLES: |
| DATOS DE IDENTIFICACIÓN:* Nombre completo.
* Domicilio.
* Lugar de nacimiento.
* Fecha de nacimiento.
* Nacionalidad.
* Edad.
* Número de teléfono.
* Estado civil.
* Correo electrónico.
* Identificación oficial o Institucional.
* Identificación del Representante Legal.

DATOS FISCALES:* Clave Única del Registro de Población (CURP).
* Registro Federal de Contribuyentes (RFC).
* Domicilio Fiscal.
* Razón Social.
* Marca Comercial.

DATOS ACADEMICOS:* Titulo o cédula profesional.
* Comprobante de estudios del último nivel alcanzado.

DATOS PATRIMONIALES:* Datos de catastro.
* Bienes muebles.
* Bienes inmuebles.
* Datos bancarios.
* Datos de créditos.

DATOS DE TERCEROS: * Nombre de los beneficiarios.
* Números telefónicos.
* Datos de terceros relacionados con el servidor público.

DATOS LABORALES:* Cargo.
* Puesto.
* Número de plaza.
 | DATOS SENSIBLES:* Fotografía.
* Firma.
* Sexo.
* Rasgos físicos.
* Imagen en la grabación.
* Discapacidad.

\* Datos biométricos:* Huella dactilar.
* Reconocimiento facial.
* Tipo de sangre.

\* Datos de salud:* Certificado médico.
 |
| Finalidades de los Datos Personales: |
| Sus datos personales serán utilizados para las siguientes finalidades:Es la presentación, creación, modificación, adición y derogación de las leyes que le correspondan según su esfera de competencia. También ejercen actividades de carácter administrativo, jurisdiccional y de control financiero o presupuestal. |
|  Formato para la obtención de los Datos Personales: |
| Dichos datos podrán ser recabados, directa o indirectamente, por medios electrónicos o por escrito. |
| Ciclo de Vida de los Datos Personales: |
| * Obtención.
* Uso.
* Almacenamiento.
* Bloqueo.
* Supresión.
 |
| V.- Estructura y Descripción ( tipo de soporte y descripción del lugar ) |
| Tipo de Soporte Físico:  | Tipo de Soporte Electrónico: |
| Descripción: | Descripción: |
|  FoldersArchiverosAnaqueles | Calipso ICON-GWord Sí declaroExcelNubeCarpetas compartidasUsbCdServidor público.Resguardadas en el equipo de computo del administrador responsable. |
| Características del lugar donde se resguardan: | Características del lugar donde se resguardan: |
| Se localizan en el área de archivo de trámite de cada sala de diputados.  | Se localiza en el área de atención al público de la sala de diputados y en los servidores del congreso del estado de Jalisco. |
| VI.- Transferencia de Datos Personales |
| Transferencia de Datos Personales de Soporte Físico: |
| Opciones de almacenamiento: | Medidas de Seguridad: |
| Se transfiere información y documentación en sobre cerrado y sellado.USBDISCOSFOLDERS | El envío de la transmisión de datos personales se realiza a través del mensajero oficial del Congreso del Estado de Jalisco.En el caso de archivos físicos se inserta la Leyenda de “Protección de Datos Personales” y/o urgente y se da instrucción para que la entrega se realice en propia mano. Previa acreditación con identificación oficial; La documentación se entrega previo acuerdo con el destinatario de la manera que se debe recibir esa información y en caso de que no se encuentre quien o quienes pueden recibir. Cualquier tipo de anomalía, irregularidad es reportada de inmediato al emisor para su conocimiento y seguimiento.Acuse de recibido: Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.El paquete con datos personales en soportes físicos viaja debidamente sellado y cerrado.  |
| Transferencia de Datos Personales de Soporte Electrónico : |
| Opciones de almacenamiento: | Medidas de Seguridad: |
| Correo electrónico.Archivos electrónicos. | Para el caso de los archivos electrónicos que contienen datos personales se utilizan contraseñas, archivos electrónicos protegidos mediante candados.Acuse de recibido electrónico: Deberá confirmar si el destinatario recibió el archivo electrónico que contenga datos personales. |
| Encargado de las Transferencias de Datos Personales: |
| VII.- Resguardo de los Soportes físicos y electrónicos de los Datos Personales |
| RESPONSABLE DESIGNADO POR EL DIPUTADO O DIPUTADAanexo 1.- bitácora de transferencia |
| Descripción del Resguardo de los Datos Personales en Soportes Físicos: |
| FoldersArchiverosAnaquelesSe almacenan dentro de la oficina del Administrador Responsable. |
| Descripción del Resguardo de los Datos Personales en Soportes Electrónicos |
| CARPETAS COMPARTIDASNUBEEXCELPROYECTO 32La base de datos personales se almacena en el disco duro del equipo de computó dentro de la oficina del Administrador Responsable.  |
| Nombre del Responsable del Resguardo de los Datos Personales |
| RESPONSABLE ASIGNADO POR EL DIPUTADO O DIPUTADA |
| VIII.- Bitácoras de acceso, Operación Cotidiana y Bitácoras de vulneraciones |
| I.- Bitácora en Soporte físico |
| *Los Datos que se registran en la Bitácora:* |
|

|  |
| --- |
| BITACORA DE VULNERACIONES |
| \* Fecha en que ocurrió la vulneración.\*El motivo de la vulneración.\* Acciones correctivas implementadas de forma inmediata.\* Acciones correctivas implementadas de forma definitiva. |

A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales. |
| Lugar de Almacenamiento: | Medidas de Seguridad: |
| *Es resguardada por el área la sala de Diputado o Diputadas.* | *Solo personal autorizado tiene acceso y se encuentra bajo llave.* |
| II.- Bitácora en Soporte Electrónico: |
| *Los Datos que se registran en la Bitácora:* |
|

|  |
| --- |
| BITACORA DE ACCESO Y OPERACIÓN COTIDIANA |
| Quien recibe o captura.Fecha en que se recibe.Quien entrega.Tipo de documento que se entrega.Referencia del documento que se entrega.Número de OICQuien suscribe el documento.Quien hace entrega del documento al Responsable del área. |

  |
| Lugar de Almacenamiento: | Medidas de de Seguridad: |
| En el programa de ExcelA la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales. | Esta resguardada con contraseña y nombre de usuario.La base de datos personales se almacena en el disco duro de una PC dentro de la oficina del Administrador Responsable. |
| IX.- Análisis de Riesgo |
| Nivel de riesgo bajo, toda vez que solamente una persona tiene acceso a ambos soportes de almacenamiento.El nivel de riesgo es bajo, toda vez que es muy poco el personal que tiene acceso a los soportes de almacenamiento de los datos personales.Las medidas de seguridad física con las que se cuenta actualmente son cerraduras. Se tiene restricciones de entrada (solo personal autorizado) debido a que solo el personal de las Jefaturas tiene acceso al documento.Las bases de datos de la información están protegidas mediante la contraseña de la computadora. El sistema utilizado cuenta con diversas medidas de seguridad. Solo personal autorizado puede ingresar a las bases de datos, cuenta con servicios denegados para el personal.

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE DATO | NIVEL DE RIESGO INHERENTE | VOLUMEN DE TITULARES | NIVEL DE RIESGO POR TIPO DE DATO |
|  DATOS PERSONALES DE IDENTIFICACIÓN. | BAJO | 5K  | 1 |
| DATOS PERSONALES DE AUTENTICACIÓN. | MEDIO | 5K  |  1 |

|  |  |  |  |
| --- | --- | --- | --- |
| DATOS FISCALES |  MEDIO |  5K |  1 |
| DATOS BANCARIOS Y DE CREDITO. |  REFORZADO |  5K |  4 |
| DATOS LABORALES Y ACADÉMICOS. |  BAJO |  5K | 1 |
| DATOS DE TERCEROS. |  BAJO |  5K |  1 |
| DATOS SENSIBLES. |  ALTO |  5K  | 3 |

 |
| X.- Análisis de Brecha |
| Para la prevención de una posible vulneración a los datos personales resguardados en el área de sala de Diputados y de Diputadas se realizara lo siguiente:\* Con respecto al personal, concientizarlos en materia de seguridad de datos personales y sus implicaciones.\* Mantener bajo llave los formularios en formato físico previo la entrega final del turno al Responsable de los Datos Personales.\* Mantener bajo llave los formularios en forma física por parte del Administrador Responsable de esta unidad.\*Mantener bajo llave los expedientes de clasificación de información.\* Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.\* Triturar todos los documentos físicos que contengan datos personales y ya no sean útiles y/o necesarios para las actividades laborales, así como borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo, los documentos o archivos electrónicos, garantizando la completa eliminación de los datos personales que ya no sean necesarios tratar por ese medio.\* Notificar de manera inmediata al área de Dirección de Apoyo Informático del Congreso del Estado de Jalisco, los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, a fin de evitar pérdida, robo, eliminación o alteraciones de información que contengan datos personales, así como la asignación de una nueva contraseña o clave.\* No difundir, transmitir ni compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos nos sean divulgados de manera no autorizada.\* Procurar solicitar acceso a los sistemas de información de tratamiento de datos personales únicamente al personal que por sus funciones y facultades laborales los requieran, a fin de mantener una adecuada segregación de funciones, restricciones de acceso y tratamiento de esos datos.\* Notificar las bajas de accesos a los sistemas de información de tratamiento de datos personales, a fin de restringir el acceso a dichos datos por personal no autorizado y que ya no forman parte del Congreso del Estado de Jalisco.\* Limitar el número de personas que tengan acceso a archivos físicos que contengan datos personales.\* Transferir los archivos físicos a bases electrónicas para evitar la pérdida de información con motivo de amenazas del tipo no intencionales.\* Notificar sobre los cambios del personal que manejen archivos físicos que contengan datos personales. |
| XI.- La Gestión de Vulneraciones |
| La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Las vulneraciones de seguridad afectan los sistemas relacionados con los datos personales en cualquier fase de su tratamiento; afecta los derechos patrimoniales o morales de los titulares de los datos personales.Se considera como vulneraciones de seguridad, las siguientes:A).- La pérdida o destrucción no autorizada.B).- El robo, extravió o copia no autorizada.C).- El uso, acceso o tratamiento no autorizado.D).- El daño, la alteración o modificación no autorizada.Por el momento no se han sufrido vulneraciones, sin embargo en caso de que suceda, se levantara una bitácora de las vulneraciones con los siguientes datos:

|  |
| --- |
| BITÁCORA DE VULNERACIONES |
| \* Fecha en que ocurrió la vulneración.\*El motivo de la vulneración.\* Acciones correctivas implementadas de forma inmediata.\* Acciones correctivas implementadas de forma definitiva. |

La notificación de la vulneración se debe informar en un plazo de 72 horas al Titular de los datos personales de manera directa ( por teléfono, correo electrónico o en persona) , al encargado de la Unidad de Transparencia y al Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco; a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos; con la siguiente información:

|  |
| --- |
| NOTIFICACIÓN DE LA VULNERACIÓN |
| \*La naturaleza del incidente: Descripción de la vulneración de manera muy sencillas y general el incidente ocurrido, en qué consistió, el periodo en el que se desarrolló. No se debe dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.\*Los datos personales comprometidos.\*Las recomendaciones a los titulares: El listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración. \*Las acciones correctivas realizadas de forma inmediata: Descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.\*Los medios donde puede obtener mayor información al respecto. |

En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, si fuese el caso, afecto de evitar que la vulneración se repita. Una vez recibida la notificación el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco por parte del responsable, podrá realizar las investigaciones previas a que haya lugar con la finalidad de allegarse de elementos que le permitan, en su caso, iniciar un procedimiento de verificación en términos de los dispuesto en la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.**Anexo 1.****Bitácora de transferencia.****Anexo 2.****Formato de identificación de incidentes. (Vulneraciones a los Sistemas de Información y Bases de Datos).****Anexo 3.****Lista de alertas de seguridad.** |
| XII.- Medidas de Seguridad Físicas de las Instalaciones donde se resguardan los Datos Personales |
| * Filtros de seguridad al ingreso de la oficina
* Oficinas restringidas
* Oficinas bajo llaves
* Archiveros bajo llaves
* Notificaciones por estrados, se omiten datos sensibles
* Acuerdo de confidencialidad.
* Inventario de Archivos.
 |
| XIII.- Control de Identificación y Autentificación de Usuarios |
| Soporte Físico: |
| \* GAFETE DEL SERVIDOR PÚBLICO: Adscrito a la sala de Diputados y Diputadas:Nombre. Cargo.Número de empleado.Domicilio y teléfono de la Institución.Firma.Fotografía. |
| Soporte Electrónico:  |
| Nombre de usuario.Contraseña.Del equipo de cómputo donde se almacena la base de datos electrónica. |
| XIV.- Procedimiento de Respaldo y Recuperación de Datos Personales |
| Datos personales en Soporte Físico: |
| *Expedientes que se generan y se resguardan bajo llave en al archivo de trámite*. |
| Datos Personales en Soporte Electrónico:  |
| En expedientes se respaldan, para su recuperación se escanean y se almacenan en discos duros de la sala de Diputados y Diputadas.Se resguardan en servidores públicos y se almacenan en los discos duros de la.Sala de Diputados y Diputadas. |
| XV.- Plan de Contingencia |
| El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información por los daños producidos por hechos naturales o por el hombre.Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en: • Leves (caídas de energía de corta duración, fallas en disco duro, equivocaciones, daño de archivos, acceso no autorizado etc.) • Severas (Destrucción de equipos, incendios, inundaciones, daño de equipo, robos, etc.Existen distintos tipos de riesgos: • Riesgos Naturales (Mal tiempo, terremoto, inundaciones, etc.) • Riesgos tecnológicos (Incendios eléctricos, fallas de energía y accidentes de transmisión y transporte). • Riesgos sociales (Actos terroristas, desordenes, entre otros).CLASIFICACIÓN DE LA CONTIGENCIA:\* GRADO 1: Son las más bajas que van desde fallas eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el personal del Congreso del Estado de Jalisco.\* GRADO 2: Requieren del apoyo del personal del Congreso del Estado de Jalisco, como del apoyo de bomberos y protección civil.\* GRADO 3: Son contingencias que por su alcance pueden afectar severamente la operatividad del Congreso del Estado de Jalisco y se requiere además del apoyo externo. CONSIDERACIONES PRINCIPALES:\* Se debe hacer 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.\* Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestros (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).\* Reunión con las comisiones o brigadas de las áreas de la Municipalidad (capacitación y evaluaciones).\* Revisión del plan e integración de las recomendaciones y decisiones adoptadas con las lecciones aprendidas del ejercicio.\* Difusión del documento del plan de contingencia una vez aprobado.PLAN DE CONTIGENCIA ANTE SINIESTROSINCENDIO.*Grado de negatividad: Muy severo.**Frecuencia de evento: Aleatorio.**Grado de impacto: Alto.*En el Congreso del Estado de Jalisco, se encuentran diferentes puntos donde se pueden conjuntar los tres elementos requeridos para formar el “Triangulo de Fuego”:1.- Oxigeno: Este se encuentra el aire libre en el medio ambiente.2.- Combustible: Se constituye principalmente por la acumulación de papel de diferentes usos, tales como el material de oficina (hojas, carpetas, libretas, expedientes, documentación, libros, etc.).3.- Calor: se ubica en contactos eléctricos, motores (ventiladores, enfriadores de agua, fotocopiadoras, computadoras) y otro tipo de electrodomésticos como cafeteras, hornos de microondas.El fuego provoca destrucción y quemaduras, principalmente en aquellos compuestos de materiales orgánicos.

|  |
| --- |
| INCENCIOS |
| Medidas preventivas en caso de incendios | Sobre el resguardo de la información en caso de incendio | Durante el incendio | Después del incendio |
| \* Asegurarse de mantener apagados durante la noche todos los equipos electrónicos y electrodomésticos. (Desconectarlos sin tirar de los cables).\* No sobrecargar los contactos eléctricos, desconectando los que no se necesitan.\* Conocimiento básico para el personal sobre primeros auxilios.\* Contar con detectores de humo.\* Mantener los cables fuera de las zonas de paso o protegidos con canaletas.\* No colocar vasos con líquidos sobre los aparatos electrónicos y electrodomésticos.\* Si se detecta cualquier anomalía o deterioro en las instalaciones eléctricas o de protección contra incendios, comunicarlo al responsable del área de mantenimiento.\* No obstaculizar en ningún momento las salidas de evacuación, así como las señalización y acceso a extintores. | \* Respaldar la información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es lugares cercanos a los extintores.\* Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube). |  \* Ante eventos como incendios, inundaciones o sismos, es primordial salvar la vida humana.\* Ubicar los extintores cerciorarse de saber usarlos y que estos sean utilizables.\* Si se detecta fuego, calor o humo anormales, dar la voz de alarma inmediatamente.\* En caso de incendio no abrir puertas y ventanas, el aire es factor para propagación del fuego.\* En caso de incendio pequeño, se procurará apagarlo, mediante un extintor. Si el fuego es de origen electrónico no se deberá intentar apagarlo con agua.\* Si es un incendio que no puede controlar usted mismo llamar a los bomberos.\* No se pierda tiempo buscando objetos personales y salga del inmueble lo antes posible; utilizando las escaleras no el ascensor.\* Permanecer en el punto de reunión.\* Si hay gas o humo humedezca un trapo y cubra su nariz y boca.\* Si su ropa se enciende; tírese al piso y ruede lentamente. |  \* Ingresar al área del siniestro hasta que las autoridades lo determinen.\* Ventilar la zona afectada, una vez apagado el incendio y previa autorización para ingresar.\* Realizar en su caso, un levantamiento de inventario de la documentación dañada. |

TERREMOTO O SISMO.Un sismo o terremoto,**es el movimiento que se da en forma natural y que sacude la superficie de la tierra.** Dicha actividad se produce, precisamente, en las capas que se encuentran en el interior de la Tierra. Los sismos pueden ser muy leves o provocar grandes daños a las propiedades y a las personas, animales y plantas que habitan en una región determinada.El daño ocasionado por un terremoto puede dañar y debilitar la estructura del edificio, la interrupción de servicios básicos, así como provocar incendios. Por lo tanto, mantener la calma y protegerse eficientemente es lo primordial. El siniestro puede provocar que las actividades se interrumpan por unas horas o hasta por un día completo.

|  |
| --- |
| TERREMOTOS O SISMOS. |
| Medidas preventivas en caso de sismos. | Sobre el resguardo de la información en caso de sismos. | Durante el sismo. | Después del sismo. |
| \* No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia.\* ubicar los muebles de archivo y objetos pesados que puedan caer al momento de un sismo y notificarlo al brigadista del Comité de Protección Civil del Congreso del Estado de Jalisco.\* Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas.\* Contar con un plan de evacuación y realizar simulacros de manera continua.\* Si se cuentan con anaqueles, los objetos pesados se colocan hasta el final.\* Localizar los lugares seguros en cada cuarto; bajo mesas solidas sólidas y escritorios resistentes.\* Contar con un botiquín de primeros auxilios. | \* No encender artículos electrónicos en la zona de archivos, evitando producir una descarga.\* Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube). | \* Mantener la calma y ubicar en una zona segura.\* No correr, no gritar, no empujar al momento de desalojar el inmueble.\* Procurar estar alejado de balcones, ventanas, lámparas, canceles, objetos calientes, libreros, gabinetes; así como de lugares donde se puedan desprender objetos.\* Si es posible cerrar llaves de gas, desconecte la alimentación eléctrica y no encender fuego.\* Permanecer en el punto de reunión previamente establecido, hasta que el movimiento pase.\* No utilizar los elevadores. | \* Ingresar al área del siniestro hasta que las autoridades lo determinen.\* Se debe realizar las instalaciones eléctricas y de gas principalmente para evitar un desastre secundario.\* Realizar en su caso, un levantamiento de inventario de la documentación dañada.\* Evite pisar cables que hubieran quedado caídos o sueltos. |

LLUVIAS EXTREMAS O FUGAS DE AGUA.Durante la temporada de lluvias se presentan algunas circunstancias que provocan encharcamientos, inundaciones o fugas en vialidades; lo anterior tiene como origen, entre otros, la saturación del drenaje y escurrimientos de agua hacia partes bajas de la zona, lo que provoca marcas sobre materiales porosos, protuberancia de materiales orgánicos, oxidación de metales, roturas y desprendimiento de papel.

|  |
| --- |
| INUNDACIONES POR LLUVIA O FUGA DE AGUA |
| Medidas preventivas en caso de inundación por lluvia o fuga de agua | Sobre el resguardo de la información en caso de inundación por lluvia o fuga de agua | Durante la inundación por lluvia o fuga de agua | Después de la inundación por lluvia o fuga de agua |
| \* Realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias estos para evitar goteras. \* Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso, respetando al menos, una altura de 10 a 15 cm de los archiveros\* La instalación de grifos que se cierren adecuadamente.\* Que la ubicación de las válvulas de control de flujo (llave de paso) sea ampliamente conocida por el personal. | \* Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local del archivo.\* Inmediatamente colocar papel secante en cada hoja de los expedientes.\* Si un documento se moja en su totalidad se puede realizar la congelación del mismo para su recuperación, debe realizarlo un especialista (restauración). \* Los documentos mojados serán extendidos sobre mesas o anaqueles para su secado por ventilación natural y/o artificial. No debiendo exponerse al calor, ni de manera directa a los rayos solares. | \* Desconectar servicios de luz, gas y agua.\* Evitar tocar o pisar cables eléctricos.\* Mantener la calma y ubicar en una zona segura.\* No correr, no gritar, no empujar al momento de desalojar el inmueble. | \* Evacuar los documentos afectados hacia áreas ventiladas.\* Realizar en su caso, un levantamiento de inventario de la documentación dañada.\* Ventilar las áreas afectadas después de la inundación.\* Ingresar al área del siniestro hasta que las autoridades lo determinen.\* Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizado en caso de emergencia, y si no hubiere mediante esponjas, baldes, recogedores, etc. |

*PROCEDIMIENTO DE CONGELACIÓN DE LOS DOCUMENTOS AFECTADOS:*Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recupéralos. A continuación se describe este procedimiento para recuperar los documentos humedecidos:1.- Se introduce la obra en una bolsa de polietileno con cierre de cremallera o termosellable. Es muy importante envolver el libro, expediente o documentación en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la congelación se realice en forma correcta, se debe dejar un amplio espacio entre los documentos, libros o expedientes.2.- La cámara de congelación debe alcanzar una temperatura de -20 °C. En un proceso acelerado de descenso de la temperatura el tratamiento será más efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe depositar el documento a restaurar en la cámara de congelación hasta que esta haya alcanzado dicha temperatura, para evitar la aclimatación de los organismos.3.- El tratamiento debe durar como mínimo 72 horas, dependiendo del grosos del documento y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas.4.- Los documentos se ha de descongelar de forma paulatina sin ser extraída del envoltorio, hasta alcanzar el equilibrio con la temperatura ambiente. Una vez congelada y alcanzado el equilibrio, el envoltorio se puede retirar.MANIFESTACIONES:En la ciudad de Guadalajara, Jalisco existen numerosos actos de manifestación, los cuales pueden interrumpir las actividades en las instalaciones del Congreso del Estado de Jalisco. Por ello se debe coadyuvar con el Comité de Protección Civil, en el caso de observar la proximidad de un contingente o de grupo de personas externas al inmueble con actitud dolosa.Por lo general, los disturbios y manifestaciones populares están vinculados a riesgos sistémicos y, en la gran mayoría de los casos, sus desencadenantes son difíciles de detectar con anticipación.

|  |
| --- |
| MANIFESTACIONES. |
| Medidas preventivas en caso de manifestaciones | Sobre el resguardo de la información en caso de manifestaciones  | Durante la manifestación | Después de la manifestación. |
| \* Establezca un sistema de información o alerta temprana que permita identificar fechas y horas de eventos que eventualmente pueden considerarse disturbios o manifestaciones potenciales.\* Establezca una línea directa de comunicación con el Departamento de Policía y Bomberos. \* Desarrolle y capacite un equipo de respuesta rápida para eventos perturbadores del orden, incluya personal de seguridad y vigilancia debidamente preparado para actuar ante tales situaciones. ̤\* Establezca rutas seguras de acceso y salida para la movilización de empleados y bienes.̤\* Asegúrese de que los sistemas de protección contra incendios y todos sus componentes estén operativos.  \* Instale protecciones en ventanas y aberturas en fachadas. \* Asegure que cadenas, candados, rejas, cerraduras, puertas y portones estén en buenas condiciones.\* Proteja tuberías, conductos y válvulas de los sistemas de protección contra incendios que estén expuestos y cerca de las vías públicas. \* Por la noche, ilumine las áreas externas de los edificios, especialmente en los puntos de acceso y ventanas, además de garantizar patrullas autorizadas para la seguridad de la propiedad. |  \* Si el archivo tiene cerradura, asegurarse que quede bajo llave. | \* Dar aviso al Comité de Protección civil, de la presencia de un contingente, o de grupos de personas externas al interior del inmueble.\* Alejarse del lugar donde se encuentren los manifestantes e invitar a las personas que están con usted hacer lo mismo.\* No caer en provocaciones ni enfrentar a los manifestantes.\* En caso de ser necesario permanecer al interior de las instalaciones por un largo periodo de tiempo o en su caso, salir de las instalaciones de forma rápida y discreta. | \* Realizar en su caso, un levantamiento de inventario de la documentación dañada.\* Una vez que se haya verificado la seguridad de las áreas, edificios, equipos y estructuras, comience las actividades de limpieza de inmediato. ̤\* Compruebe que los sistemas de protección contra incendios estén en buenas condiciones de funcionamiento.\* Repare de inmediato si se identifica un defecto o daño en cualquier sistema de protección. |

ROBOROBO COMÚN DE EQUIPOS:\* En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias, así como un botón de pánico por medio de una App instalada en el celular.AMENAZAS INFORMÁTICAS:Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopiadoras etc.; y tener contacto con proveedores de software, hardware y medios de soporte.\* Prevención de falla de los equipos: Se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún remplazo inmediato.\* Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores/ reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la perdida de información importante.HACKEO INFORMÁTICO:Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:CAMBIAR CONTRASEÑAS:\* Debe tener al menos ocho caracteres.\* No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del Congreso del Estado de Jalisco.\* Debe ser muy distinta a tus contraseñas previas.\* No debe contener palabras completas.\* Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales.Mientras se esté conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe desconectar el cable de la red lo antes posible.POSTERIORMENTE:\* Contactar al personal de soporte para que retire del aire la página.\* Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.MANTENER LA MISMA DIRECCIÓN WEBCuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía.Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

|  |
| --- |
| *PLAN DE CONTIGENCIA ANTE SINIESTROS**Medidas de prevención y conservación de los archivos* |
| \* El archivo general debe situarse en el primer piso del edificio (no sótanos o pisos superiores del edificio).\* Espacios con luz natural y sin humedad.\* Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad. (Un archivo de muebles dispares da la sensación de desorden).\* Evitar archivar documentación cerca de fuentes de humedad y de 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 a su vez la acumulación de humedad y proliferación de plagas).\* Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.\* Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.\* Contar con extintores específicos para apagar fuego por quema de papel. (Se deben de verificar periódicamente, recargados y colocados de nuevo en su lugar).\* Identificar las rutas de evacuación, así como las salidas de emergencia.\* Conservar los documentos y expedientes organizados, e inventariados, para el supuesto de tener algún daño, saber la cantidad exacta a restaurar.\* Contar con instalaciones de sistemas de detección de humo.\* El personal adscrito a los archivos debe recibir capacitación obligatoria periódica en el uso de extintores. |

 |
| XVI.- Técnicas de Supresión y Borrado de los Datos Personales |
| Desmagnetización | - |
| Destrucción Física | SI |
| Sobre-escritura | SI |
| Descripción de la técnica: |
| El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena.1.- Trituración: Las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos.Los medios ópticos de almacenamiento (CD) serán destruidos por trituración de corte transversal.2.- Depuración de los medios de almacenamiento electrónicos en formatos generados word para la captura de datos personales, consistente en eliminar la información que ya no se considere necesaria para útil para el fin en que se capturó en el archivo.3.- La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento.Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables. |
| XVII.- Plan de Trabajo |
| 1.- De manera permanente se mantiene orientación y su previsión con el personal del área para dar a conocer la importancia de la protección de datos personales.2.- Solicitar apoyo para capacitaciones en materia de Protección de Datos Personales al lTEl.3.- Concientizar a los servidores públicos de la responsabilidad en el tratamiento y protección de datos personales. |
| 4.- Solicitar apoyo para mejorar la seguridad física de la oficina.5.- Revisiones periódicas en instalaciones donde se resguardan los datos personales (anual) y llevar a cabo informes anuales de la revisión y mejora.6.- Solicitar al área de Dirección de Apoyo informático aumento de protección constante en las bases de datos electrónicas. |
| XVIII.- Mecanismos de monitoreo y Revisión de las Medidas de Seguridad. |
| Al momento de ejecutar los procedimientos relativos al manejo de los datos personales en donde se van detectando áreas de mejora, perfeccionando cada vez la seguridad y protección de los datos personales.Revisiones periódicas en instalaciones y sistemas donde se resguardan los datos personales, realizando informes anuales de la revisión y mejora. |
| XIX.- Programa General de Capacitación |
| La capacitación continua a los servidores Públicos de las salas de Diputados y Diputadas permite mejorar y realizar de manera más eficiente las actividades en colaboración con la unidad de Transparencia.De conformidad con el artículo 87, párrafo 1, fracción VII de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, es atribución del Comité de Transparencia:*"VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales;"* |
| De igual forma el artículo 90, párrafo 1, fracciones IV y XIII de la citada Ley, señala que es atribución del Instituto de Transparencia:*"IV. Capacitar a los sujetos obligados en sus obligaciones respecto el tratamiento de datos personales en su posesión;**XIII. Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la presente Ley;"*. |



ANEXOS

**ANEXO 1.- BITÁCORA DE TRANSFERENCIAS**

**BITÁCORA DE TRANSFERENCIAS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **FECHA** | **MEDIO** | **DATOS PERSONALES TRANSFERIDOS** | **RECEPTOR** | **PERSONA QUE RECIBE** | **AUTORIZACIÓN** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**ANEXO 2.- A.- FORMATO DE IDENTIFICACIÓN DE INCIDENTES. (VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS).**

**VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS**

|  |  |
| --- | --- |
| **FECHA DEL INCIDENTE** |  |
| **NOMBRE** |  |
| **CARGO** |  |
| **AREA** |  |
| **RESPONSABLE DEL ÁREA** |  |
| **CAUSA DE LA VULNERACIÓN** |  |
| **SISTEMA DE INFORMACIÓN O DATOS VULNERADO** |  |
| **CANTIDADES DE TITULARES DE LOS DATOS PERSONALES** |  |
| **SOPORTE DE LA INFORMACIÓN VULNERADA** | **FISICO** | **ELECTRÓNICO** | **MIXTO** |
|  |  |  |
| **SELECCIONE EL TIPO DE VULNERACIÓN** | **PERDIDA O DESTRUCCIÓN NO AUTORIZADA** |  |
| **ROBO, EXTRAVIO O COPIA NO AUTORIZADA** |  |
| **USO, ACCESO O TRATAMIENTO NO AUTORIZADO** |  |
| **DAÑO, ALTERACIÓN O MODIFICACIÓN NO AUTORIZADA** |  |
| **TIPO DE DATOS PERSONALES COMPROMETIDOS** | **IDENTIFICATIVOS** |  |
| **LABORALES** |  |
| **TRÁNSITO Y MOVIMIENTOS MIGRATORIOS** |  |
| **ACADÉMICOS** |  |
| **PROCEDIMIENTOS ADMINISTRATIVOS O JUDICIALES** |  |
| **PATRIMONIALES** |  |
| **SALUD** |  |
| **IDEOLÓGICOS** |  |
| **DE ORIGEN** |  |
| **CARACTERÍSTICAS PERSONALES** |  |
| **VIDA SEXUAL** |  |
| **UBICACIÓN** |  |
|  |  |  |
| **NOMBRE Y FORMA DE QUIEN REPORTA.** | **NOMBRE Y FIRMA DEL ADMINISTRADOR DEL SISTEMA.** | **NOMBRE Y FIRMA DEL TITULAR DEL ÁREA.** |

**ANEXO 2.- B.- Formato de identificación de incidentes. (Vulneraciones a los Sistemas de Información y Bases de Datos).**

**VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS**

|  |  |
| --- | --- |
| **FECHA DEL INCIDENTE** |  |
| **NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN.** |  |
| **CARGO** |  |
| **ÁREA** |  |
| **NÚMERO DE INVESTIGACIÓN** |  |
| **LA INFORMACIÓN VULNERADA ESTA REGISTRADA EN EL DOCUMENTO DE SEGURIDAD** | **SI** |  | **NO** |  |
| **EN CASO DE QUE LA INFORMACIÓN NO ESTUVIERA VULNERADA, SOLICITE AL RESPONSABLE DEL ÁREA UN INFORME AL RESPECTO CON EL OBJETO DE RESPONDER EL CONTENIDO DEL APARTADO A.** |
| **APARTADO A** |
| **FECHA EN QUE SE CREO EL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADA** |  |
| **FUNDAMENTO LEGAL PARA OBTENCIÓN DE LOS DATOS PERSONALES** |  |
| **RESGUARDO DE LOS SOPORTES** |  |
| **USUARIOS** |  |
| **MEDIDAS DE SEGURIDAD FISICAS TÉCNICAS Y ADMINISTRATIVAS APLIACADAS** |  |
| **LAS CAUSAS ENUNCIADAS EN EL FORMATO A** |  |
| **LO QUE EL TITULAR DEL ÁREA CONSIDERE PERTINENTE** |  |
| **APARTADO B** |
| **ADMINISTRADOR DEL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADO** |  |
| **USUARIOS DEL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADOS** |  |
| **LOS HECHOS DE MODO, TIEMPO Y LUGAR ENUNCIADOS EN EL FORMATO**  |  |
| **RESGUARDANTE SOPORTE FISÍCO O ELECTRÓNICO VULNERADO** |  |

**ANEXO 3.- EJEMPLOS DE ALERTAS DE SEGURIDAD.**

Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos, se habla de un incidente de seguridad. En la siguiente tabla se enlistan diferentes categorías de incidentes de seguridad.

|  |  |
| --- | --- |
| **CATEGORÍA** | **EJEMPLOS** |
| Desastre natural( más allá del control humano) | Terremoto, erupción de un volcán, tsunami, huracán, etc. |
| Inestabilidad social | Huelgas, terrorismo, guerra. |
| Daño físico(accidental o deliberado) | Incendio, inundación, malas condiciones ambientales (contaminación, polvo, corrosión, congelamiento), radiación o pulso electromagnético, destrucción parcial o total de medio almacenamiento físico o electrónico. |
| Falla de la infraestructura | Falla en el suministro de servicios como: energía, agua, telecomunicaciones y redes, aire acondicionado. |
| Falla técnica | Fallas de hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento. |
| Software malicioso | Diferentes categorías de software malicioso ( malware) como virus, troyanos, software de acceso y control remoto ( RTA, por sus siglas en inglés), amenazas persistentes avanzadas(APT, por sus siglas en inglés), Ransomware. |
| Ataques técnicos | Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a la fuerza.Escaneos de redes, utilización de puertas traseras en el software, intentos de accesos no autorizados, inferencia de contraseñas, ataques de denegación de servicios. |
| Incumplimiento de reglas o políticas ( accidental o deliberado) | Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas o ilegales, copia o sustracción de documentos o información no autorizada, |
| Información dañada | Sobre escritura accidental, error de captura o de almacenamiento. |
| Intercepción de información | Espionaje, intervención de comunicaciones, ingeniería social, robo, pérdida o extravío de información. |
| Divulgación de contenido perjudicial | Difusión en medios masivos de comunicación de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas. |

**ANEXO 4.- MANUAL PARA CIFRAR DOCUMENTOS**

“Cómo cifrar documentos en Word o Excel”

|  |
| --- |
|  **CONTRASEÑA PARA ARCHIVO WORD** |
| 1.- Lo primero es abrir el archivo que queramos proteger. |
| 2.- Una vez abierto, vamos a Archivo. Se da clic en Información y le damos a proteger documento, cifrar contraseña. |
| 3.- Acto seguido nos pide que pongamos una clave dos veces. En cuanto aceptemos, quedará registrada. |

Si desea revertir la situación, se hará los siguientes pasos:

\* Seguir los pasos anteriores (1,2y 3), una vez que estamos en cifrar contraseña, simplemente tendremos que borrarla y dar clic en aceptar. El archivo de Word quedará abierto nuevamente.

También podremos hacer que nuestro documento sea sólo de lectura, restringir la edición u otorgar permisos sólo a ciertos usuarios.

|  |
| --- |
| **CONTRASEÑA PARA ARCHIVO EXCEL** |
| 1.- Lo primero es abrir el archivo e ir a Archivo, Información. |
| 2.- una vez aquí dar clic en Permisos, proteger libro y cifrar con contraseña. |
| 3.- Acto seguido nos pide que pongamos una clave dos veces. El archivo estará cifrado con una contraseña. |

Para revertir la situación debemos de realizar el mismo proceso. Borrar la clave que hemos puesto y pulsar en aceptar.

**“COMO CIFRAR UN ARCHIVO”**

El cifrado de archivos ayuda a proteger los datos mediante su cifrado. Solo una disponga de la clave de cifrado correcta (por ejemplo, una contraseña) puede descifrarlos. El cifrado de archivos no está disponible en Windows 10 home.

|  |
| --- |
| **COMO CIFRAR UN ARCHIVO** |
| 1.- Haz clic con el botón derecho en un archivo o carpeta (o mantenerlo presionado) y selecciona Propiedades. |
| 2.- Selecciona el botón opciones avanzadas y selecciona la casilla de verificación Cifrar contenido para proteger datos. |
| 3.- Selecciona Aceptar para cerrar la ventana Atributos avanzados, selecciona Aplicar y luego selecciona Aceptar. |