DOCUMENTO DE SEGURIDAD DEL USO DE DATOS DEL INSTITUTO DE INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL ESTADO DE JALISCO

INTRODUCCIÓN

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos.

Aunado a dicha normatividad y de conformidad con los artículos 3° fracción XIV, artículos del 30 al 44 y a la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales Federal, se crea el presente documento de seguridad.

Desde la creación del Instituto de Información Estadística y Geográfica del Estado de Jalisco, a través de la Unidad de Transparencia, y en conjunto con los servidores públicos designados por los titulares de área que se tiene en cada área generadora de información, se han realizado acciones y actividades que tuvieron como finalidad establecer los cimientos para la creación de este documento.

Entre algunas de las actividades, destaca la aplicación de un cuestionario al personal del instituto que nos permitió identificar información básica del tratamiento al que son sometidos por cada una de las áreas de este instituto.

Este documento permitió identificar los datos personales a los que tiene acceso cada uno de los servidores públicos del IIEG, esto con la finalidad de la creación del sistema de tratamiento de datos personales sobre los mismos.

Desde la creación del IIEG, se han realizado capacitaciones especializadas en materia de protección de datos personales con la finalidad de concientizar a los servidores públicos sobre el trato lícito y adecuado de los datos personales.

Para recabar información precisa, se realizó un cuestionario a través de la Unidad Transparencia a cada una de las direcciones y coordinaciones del IIEG, con la finalidad de detectar medidas de seguridad con las que ya contaba cada área y definir posibles riesgos. Una vez contestado el cuestionario, se analizó la información recabada, lo que nos permitió la creación de las medidas de seguridad.

A partir del inventario inicial de datos personales, de las capacitaciones y diversas gestiones con cada uno de los titulares de las áreas generadoras y resguardantes de la información, se generaron cada una de las partes que integran el presente documento de seguridad, siguiendo como objetivo el propiciar la protección de los datos personales de la forma más completa, ello encaminado a lograr el adecuado tratamiento de los datos personales.

El presente documento se guiará por los principios, y conceptos que establece Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

SISTEMAS DE TRATAMIENTO O BASES DE DATOS PERSONALES

Después del inventario inicial de datos personales, de las capacitaciones, el cuestionario y diversas gestiones con los servidores públicos de todas las áreas del IIEG, se diseñaron los sistemas de tratamiento, señalados a continuación:

Sistema de tratamiento de los pagos a empleados			
Administrador	**Nombre de la persona a cargo**	**Bases de datos**	**Enumerar las bases de datos personales que formen parte del sistema**
Cargo:	**El cargo que ostenta la persona**		
Área	**Área de adscripción**		
Funciones y obligaciones	**Enumerar las funciones y obligaciones de la persona de acuerdo a su puesto.**		
Personal autorizado para tratamiento (Incluir a las personas que formar parte del sistema al tratar datos personales)			
Nombre del puesto	**Nombre de la persona**	**Bases de datos**	**Enumerar las bases de datos personales que formen parte del sistema**
Funciones y obligaciones:	**Enumerar las funciones y obligaciones de la persona de acuerdo a su puesto.**		
Tipo de datos personales pertenecientes al sistema de tratamiento de los pagos a empleados			
Inventario:	**Enlistar los datos personales que se recaban en dicho sistema.**		

Bases de datos	**Enlistar todas las bases de datos tratadas en el sistema.**	
No. De titulares	**De cuantas personas se tienen recabados datos personales en el sistema.**	
Controles de seguridad para las bases de datos	**Las formas en las que se protegen las bases de datos para evitar un acceso no autorizado.**	
Estructura y descripción del Sistema de tratamiento		
Tipo de soporte:	**Los tipos de soporte en el sistema de tratamiento**	
Características del lugar de resguardo:	**Las características físicas del lugar donde se resguardan los datos personales.**	
Programas en que se utilizan los D.P.	**El software (programas de computadora) donde se utilizan los datos personales.**	
Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales		
Físicos	**Características físicas y administrativas de los resguardos de los soportes y el nombre de la persona a quien están los resguardos.**	
Electrónicos	**Características físicas y administrativas de los resguardos de los soportes y el nombre de la persona a quien están los resguardos.**	
Las bitácoras de acceso y- operación cotidiana		
Bitácoras Físicas	**Identificación y/o lugar de almacenamiento**	
Clave de la bitácora	**Nombre de la bitácora para su identificación, el tipo de soporte, quien la resguarda y donde se almacena, así como las características del lugar de almacenamiento.**	
Bitácoras Electrónica.	**Identificación y/o lugar de almacenamiento**	
Clave de la bitácora	**Nombre de la bitácora para su identificación, el tipo de soporte, quien la resguarda y donde se almacena, así como las características del lugar de almacenamiento.**	
Las bitácoras de vulneraciones de seguridad		
ID	**Soporte**	**Responsable**
Clave de la bitácora	**Físico o Electrónico**	**Administrador del sistema**

Lo anterior tiene fundamento en:

Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipio.

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

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del IIEG que participan en el tratamiento de los datos personales derivado de sus atribuciones, al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:

1) Tener a la vista el Aviso de Privacidad.

2) Dar a conocer el aviso de privacidad al titular de los datos personales antes de la obtención de sus datos.

3) En caso de dudas y/o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.

4) Al obtener los datos personales cerciorarse de que la información esté completa, sea veraz y comprensible.

5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales.

6) Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.

7) Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

8) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

9) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Información Estadística y Geográfica del Estado de Jalisco, en el tratamiento de datos personales.

10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

11) Tomar, cuando menos una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público involucrado en el tratamiento de datos personales deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al documento de Seguridad del Instituto de Información Estadística y Geográfica del Estado de Jalisco en el tratamiento de datos personales.

2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que aplica.

3) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

4) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.

5) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

6) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

7) Tomar, cuando menos una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Información Estadística y Geográfica del Estado de Jalisco, en el tratamiento de datos personales.

2) Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.

3) Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

4) Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.

5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

6) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

8) Tomar, cuando menos una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

9) Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.

10) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.

11) Informar a la Unidad de Transparencia sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

12) Acudir a la Unidad de Transparencia en caso de asesoría sobre el tratamiento de datos personales.

13) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

14) Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

15) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público responsable de cada sistema, o en su caso, el titular de cada dirección o coordinación responsable de cada sistema deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Instituto de Información Estadística y Geográfica del Estado de Jalisco, en el tratamiento de datos personales.

2) Implementar las medidas de seguridad que establece el documento de seguridad.

3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

4) Tomar una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

5) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la unidad de Transparencia.

6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.

7) Informar a la Unidad de Transparencia sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

8) Monitorear la implementación de las medidas de seguridad.

9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

10) Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la Unidad de Transparencia.

12) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Unidad de Transparencia.

13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, la Unidad de Transparencia y el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de

Jalisco, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.

2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

3) Requerir anualmente a las dependencias o áreas responsables que tratan datos personales a través de la Unidad de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

Son obligaciones de la Unidad de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior del Instituto de Información Estadística y Geográfica del Estado de Jalisco el aviso de privacidad y el documento de seguridad.

2) Revisión física anual a las áreas del instituto sobre el tratamiento de datos personales y la implementación de medidas de seguridad.

3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.

4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

LA ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO Y/O BASES DE DATOS PERSONALES, SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

Los datos personales que obran en documentos físicos son resguardados en escritorios y archiveros de cada una de las unidades del instituto, mientras que los datos personales que son procesados y digitalizados se almacenan en los sistemas electrónicos.

- NOMIPAC

- Sistema de checado

NOMIPAC y el Sistema de Checado contienen datos personales con un nivel de riesgo bajo, Medio y Alto, información necesaria para llevar a cabo los procesos de administración, contratación, desarrollo y control.

El soporte físico consta de todo el mobiliario donde se almacena la información cuyo resguardo se encuentra a cargo de los titulares de cada una de las unidades del instituto. En tanto el soporte electrónico es vigilado y resguardado por la Dirección de Tecnologías de la información, instancia encargada de implementar los métodos, procesos y técnicas necesarias, con el fin de almacenar, procesar y transmitir la información que se genere en forma digital.

Estructura y características de los principales tipos de soporte con lo que cuenta el IIEG.

Hardware

Consiste en todos los medios físicos electrónicos que soportan procesos de datos personales en los que se incluyen los siguientes:

Equipo de procesamiento de datos. Equipo para el procesamiento de información personal, incluyendo los elementos que operan independientemente, __ computadoras, __ discos duros externos y __ servidores.

Equipo móvil. Equipo de cómputo portátil, por ejemplo laptops, tablet y Smartphone.

Periféricos. Equipo conectado a una computadora para la entrada y salida de datos, por ejemplo impresora, mouse y teclado.

Soportes

Consiste en todos los programas y aplicaciones que contribuyen al procesamiento de datos personales.

Soportes electrónicos. Medios electrónicos de información mediante el uso de un dispositivo electrónico como una computadora para examinar, modificar o almacenar los datos en medios de almacenamiento masivo.

Soportes físicos. Medios de información inteligibles a simple vista, que no requieren de ningún dispositivo electrónico que procese su contenido para examinar, modificar o almacenar los datos, por ejemplo, papel escrito a mano o impreso, fotografías entre otros.

Software

Consiste en todos los programas y aplicaciones que contribuyen al procesamiento de los datos personales.

Sistemas operativos. Incluye a todos los programas que funcionan como plataforma base para que operen otros programas tales como servicios y aplicaciones.

Software de servicios, mantenimiento o administración del software. Complementa a los servicios operativos y no están directamente accesibles por los usuarios o aplicaciones por ejemplo plataformas de actualización y antivirus.

Redes y Telecomunicaciones

Consiste en todos los programas y aplicaciones que contribuyen al procesamiento de los datos personales.

Sitios

Comprende todos los lugares o locaciones que contienen los activos y procesos, así como los medios físicos necesarios para operar.

Zonas. Son los espacios delimitados por barreras físicas formando divisiones dentro del ambiente interno de la organización, así como dentro de las estructuras de tratamiento de los datos personales, entre las que se encuentran oficinas, zonas de acceso restringido y zonas seguras.

Personal y Organización

Además de los encargados y responsables del tratamiento de datos personales, consiste en el resto de los sujetos involucrados en el Sistema de Gestión de Datos del Personal.

CONTROLES Y MECANISMOS DE SEGURIDAD PARA LA TRANSFERENCIA QUE, EN SU CASO, SE EFECTUEN.

El aviso de privacidad del IIEG establece que los datos recabados son única y exclusivamente para llevar a cabo los objetivos y atribuciones de este instituto. El personal tiene prohibido recabar algún otro adicional que no corresponda con las funciones encomendadas a este organismo público descentralizado.

En caso de requerirse una transferencia de datos personales, los controles y mecanismos de seguridad están supeditados a los que marca el Titulo Quinto de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

En este capítulo, el artículo 70 y 71 establecen el consentimiento y las formalidades de las transferencias, partiendo de que toda transferencia de datos personales sea nacional o internacional está sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley.

Toda transferencia deberá de formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Esta disposición no será aplicable en dos casos: 1) cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de sus atribuciones expresamente conferidas a estos; y 2) cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional completamente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homologadas, o bien, las finalidades que motivan la trasferencia sean análogas o compatibles.

Cuando se requiera transferir datos personales a terceros, el IIEG deberá asegurarse que el tercero cuente con políticas y procedimientos acordes a la Ley, en atención a cuatro criterios:

I.- El tercero cuenta con mecanismos para que el interesado pueda informarse sobre el uso y tratamiento que reciben sus datos personales;

II.- El tercero cuente con mecanismos para que el titular ejerza sus derechos de acceso, ratificación, cancelación y oposición;

III.- El tercero posea medidas de seguridad suficientes que garanticen la protección de los datos personales; y

IV.- La transferencia de datos se llevara a cabo con terceros que garanticen un adecuado nivel de cumplimiento de protección de datos.

En seguimiento a lo descrito, el articulo 72 y 73 de la ley en comento abordan las transferencias a nivel nacional e internacional, resaltando en el primer caso que el receptor de los datos personales deberá de comprometerse a garantizar su confidencialidad y únicamente los utilizara para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad; en tanto el receptor de los datos personales por el simple hecho de recibir los mismos adquiere el carácter de responsable.

El artículo 74 establece que en toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular y finalmente el artículo 75, se abordan las excepciones al consentimiento, donde se indica que el responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

EL RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS DE LOS DATOS PERSONALES.

La infraestructura física que resguarda la información consta de dispositivos y servidores alojados en sitios de comunicaciones, cuyas normas para la optimización de su funcionamiento consiste en conservar la temperatura adecuada, con mantenimiento preventivo y conectado a un no break como supresor de voltaje.

En el caso de la información almacenada en la red interna, su diseño delimita el tratamiento y seguridad a través de una red pública y otra privada. En la red pública cada usuario tiene una carpeta con permisos de editar o borrar cualquier tipo de archivo, al igual que otras áreas pueden accesar con los mismos privilegios. Por su parte, la red privada es un espacio exclusivo al que solamente los propios usuarios tienen acceso.

Por lo que ve a la información almacenada se cuenta con un resguardo de datos en los servidores internos, generado a partir de la operatividad de las plataformas y automatización de procesos, pero con acceso restringido.

LAS BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Aunque en el IIEG existen bitácoras en las que se registran los accesos de quienes ingresan a las instalaciones físicas, es necesario contemplar nuevos formatos en los que se detalle la operación cotidiana y las posibles vulneraciones a la seguridad de los datos personales en posesión de este instituto.

De acuerdo con el artículo 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, se consideran como vulneraciones de seguridad.

I. La pérdida o destrucción no autorizada

II. El robo, extravío o copia no autorizada

III. El uso, acceso o tratamiento no autorizado

IV. El daño, la alteración o modificación no autorizada.

En este sentido, las vulneraciones deberán ser reportadas dentro de una bitácora que describa la naturaleza del incidente, la fecha en que ocurrió, el motivo de la vulneración, los datos personales comprometidos y las acciones correctivas implementadas de forma inmediata y definitiva.

Bitácoras de acceso y vulneraciones a la seguridad de los datos personales.	
Fecha	
Naturaleza del incidente	
Motivo de la vulneración de la seguridad	
Datos personales comprometidos	
Acciones correctivas implementadas de manera inmediata y definitiva	

Cada una de las unidades del instituto deberá de reportar las actividades o sucesos relevantes en los que se haya visto vulnerado o alterado algún sistema de datos personales, sea físico o electrónico.

Cabe señalar que en caso de la Coordinación General de Tecnologías de la Información la bitácora tendrá que ser reportada de manera trimestral aun cuando no haya surgido una vulneración a la seguridad. Esto con la finalidad de monitorear de manera permanente los sistemas de tratamientos electrónicos del instituto, puesto que es aquí donde se pueden presentar mayores ciberataques o vulneraciones a la seguridad que protege los datos personales.

ANÁLISIS DE RIESGOS

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

1) Obtención de datos incompletos o incorrectos.

2) Omitir la notificación al titular de los datos personales del aviso de privacidad.

3) No difundir el aviso de privacidad.

4) No tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad, por no tener un consentimiento expreso.

Después de identificar dichos riesgos es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del municipio.	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información.

Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del municipio.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de los ciudadanos. Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Robo de información. Extorsión. Modificaciones no autorizadas. Robo de información.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.

Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.

Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Es importante mencionar que hasta la creación del presente documento no se han identificado o reportado vulneraciones desde las áreas generadoras de información del Instituto de Información Estadística y Geográfica del estado de Jalisco.

ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base en los cuestionarios que se hicieron a cada uno de los servidores públicos por parte de la Unidad de Transparencia a las unidades y coordinaciones generadoras de información del instituto.

Las unidades y coordinaciones reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las unidades y coordinaciones del sujeto obligado El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

GESTIÓN DE VULNERACIONES

Plan de respuesta

1) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.

2) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.

3) Llenado de Formato A (anexo 1), por parte de la persona que detectó la vulneración.

4) Llenado de Formato B (anexo 2), por parte de la Coordinación General Jurídica.

5) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.

6) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.

7) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.

8) Llenado de la bitácora de vulneraciones conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y Municipios.

MEDIDAS DE SEGURIDAD IMPLEMENTADAS MEDIDAS DE SEGURIDAD FÍSICAS

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

LAS MEDIDAS DE SEGURIDAD

De acuerdo a lo expuesto anteriormente, se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo de control	Descripción
Control de servidores públicos que recaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. (Quien recabe los datos generales para el trámite a realizar). Actualización del listado: cada 6 meses.
Control de servidores públicos que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales impartida por la UTI.
Control de servidores públicos que recaban los datos personales.	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Obtención de datos.	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad.	El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.
Aviso de privacidad.	Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del instituto, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado.

Aviso de privacidad	Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, ésta deberá contener la mención y debe dar a conocer el aviso de privacidad del Instituto, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general.
Espacio físico.	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área.
Espacio físico.	El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones.
Espacio físico.	Las llaves de las puertas de cada dependencia, deberán ser guardadas únicamente por servidores públicos del área, autorizados para poseer las llaves.
Espacio físico.	Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados.
Espacio físico.	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Resguardo provisional, durante el desahogo del trámite.	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.
Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: · No estar al alcance de los ciudadanos o servidores públicos ajenos al área. · Deberá ser un área específica para guardar los expedientes. · Este archivo debe estar bajo llave. · La llave del mismo solo puede estar en manos de un servidor autorizado para esto.

Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener lo siguiente: · Registro para anotar el nombre y puesto del servidor público autorizado. · Fecha, hora de entrada y hora de salida del archivo. · Registrar el expediente que se consultó. · Registrar el expediente que se extrae del archivo, y fecha en la que se regresa el expediente. · Firma de conformidad del servidor público que entró. · Firma de consentimiento del servidor público autorizado para llevar el control de este archivo.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal.
Control de archivos electrónicos.	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Inventarios Documentales sobre archivos entregados a la Coordinación de Gestión Documental.	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos que se mandan a la Coordinación de Gestión Documental para su resguardo en el archivo del instituto.
Transferencia de datos personales.	En caso de ser necesario y derivado de las funciones de los servidores públicos, o por requisito del trámite, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.

Archivo finalizado	Al momento de finalizar el trámite, todos los expedientes, deberán desecharse, enviarse y mandarse al archivo del Instituto, conforme a la normatividad correspondiente.

Medidas de seguridad para transferencias; transferencias al interior del sujeto obligado y a otros sujetos obligados:

1) Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.

2) El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.

3) El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.

4) El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.

5) El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.

6) El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.

Transferencias a terceros:

1) El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.

2) En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

Medidas de seguridad en caso de vulneraciones a la seguridad:

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, misma que deberá seguirse bajo el siguiente formato y ejemplo:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de forma inmediata y definitiva
30/05/2018	Huracán.	Impresión del expediente. Generar nuevo expediente electrónico.

CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Identificación	

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Se realiza una digitalización completa de la información que ingresa a través de la oficialía de partes y se almacena en discos duros. A partir de la aprobación del presente documento deberá realizarse un respaldo incremental almacenado en discos duros.

Respaldo

Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo. Se puede adquirir una aplicación de respaldo que identifica y registra la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados desde esas operaciones.

Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Instituto, atendiendo, a las recomendaciones de la Coordinación General de Archivo Sustanciación de Procesos y Unidad de Transparencia, así como de la Coordinación General Jurídica.

PLAN DE CONTINGENCIA

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que nos encontramos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios

por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evoluciona. Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DE DATOS PERSONALES

Métodos Físicos

1. Trituración mediante corte cruzado o en partículas: Utilizar las trituradoras de papel ubicadas en las diversas áreas del Instituto, que permite cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.
2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos

Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

PLAN DE TRABAJO

La existencia del documento de seguridad, busca enmarcar los deberes del Instituto de Información Estadística y Geográfica del Estado de Jalisco, para la máxima protección de datos personales, ello debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el IIEG realizará para la aplicación del presente documento de seguridad, lo anterior se realizará en base a las atribuciones establecidas en la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1) Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.

2) Se comunicará a los servidores públicos designados por sus titulares la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

3) Se buscará la participación del ITEI para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará cada 6 meses, a partir de la emisión del presente documento de seguridad:

1) Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.

2) Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para el Instituto de Información Estadística y Geográfica del Estado de Jalisco.

3) Actualizar el presente plan de trabajo.

4) Se emitirá un programa anual de capacitaciones y además se promoverá que el personal del IIEG se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Para la correcta ejecución se realizará un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúen siendo efectivas e idóneas para el IIEG.

A continuación, se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

Mecanismos de monitoreo.	Objetivo del monitoreo.
Visitas a cada una de las áreas cada 12 meses.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.

Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear y monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

EL PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado, estas serán por lo menos 1 vez al año, las fechas exactas se les notificarán a los servidores públicos designados por los titulares de área de transparencia con al menos dos semanas de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.

Las capacitaciones serán conforme a lo siguientes temas de relevancia:

Protección de datos personales.- En esta capacitación se introducirá a las novedades que brindará la Ley General de Protección de Datos Personales para poder realizar y administrar correctamente las gestiones y trámites que contienen información confidencial, así como las medidas que deben tomarse para su protección y las implicaciones que existen en caso de no proteger adecuadamente dicha información. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios.- Este módulo está dirigido para el personal interesado en aprender lo más básico en materia de protección de datos personales en apego a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios; su objetivo es introducir las bases y generalidades de esta ley, así como resolver dudas de la misma.

Medidas de seguridad de datos personales.- En esta capacitación se introducirá a las novedades que brindará la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios para poder realizar y administrar correctamente las gestiones y trámites que contienen información confidencial, así como las medidas que deben tomarse para su protección. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

Versiones públicas.- En este módulo se expondrán de manera general los lineamientos que el Sistema Nacional ha desarrollado para la correcta gestión de versiones públicas de documentos que serán entregados o publicados que contengan datos personales y su correcta realización, teniendo como objetivo principal explicar cómo se realiza una versión pública de los documentos que lo requieren y responder dudas sobre el tema que tengan los servidores públicos designados por los titulares de área de transparencia.

Solicitudes de acceso, ratificación, cancelación u oposición de datos personales .- Este módulo está dirigido para el personal del instituto que maneja datos personales y/o servidores públicos designados por los titulares de área de transparencia de cada área que da respuesta a las solicitudes de Derechos ARCO, esta capacitación tiene como finalidad instruir a los interesados como deben ser contestadas dichas solicitudes con base a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios. Teniendo como objetivo principal introducir a las bases y generalidades de esta ley, así como resolver dudas de la misma.

Sistema de manejo de protección de datos personales.- En este módulo se expondrán de manera general los lineamientos que el Sistema de manejo de datos personales en posesión del sujeto obligado, desarrollado para dar a conocer los nuevos lineamientos con respecto a este sistema, teniendo como objetivo principal explicar cómo se realizan las nuevas actividades que nos permitan desarrollar de forma precisa este sistema.

Seguimiento de medidas de seguridad.- En esta capacitación se dará seguimiento a la aplicación de medidas de seguridad en cumplimiento a la Ley General de Protección de Datos Personales para poder realizar y administrar correctamente las mismas para el debido manejo de datos personales en posesión del sujeto obligado, así como las implicaciones que existen en caso de no proteger adecuadamente dicha información. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

Sesión de dudas en materia del adecuado manejo de datos personales. - En este módulo se expondrán de manera general las posibles actualizaciones del documento de seguridad del sujeto obligado y se atenderán las dudas de los servidores públicos designados por los titulares de área en materia de transparencia de cada unidad y coordinación, para dar seguimiento y cumplimiento a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios.

ANEXO 1

FORMATO A

Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	Haga clic aquí para escribir una fecha.
NOMBRE	
CARGO	
AREA	
RESPONSABLE DEL ÁREA	
CAUSA DE LA VULNERACIÓN	
SISTEMA(S(DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERAD(O)	
CANTIDAD DE TITULARES	
SOPORTE DE LA INFORMACIÓN VULNERADA	☐ Físico ☐ Electrónico ☐ Mixto
SELECCIONE EL TIPO DE VULNERACIÓN	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada
TIPO DE DATOS PERSONALES COMPROMETIDOS	☐ Identificativos ☐ Laborales ☐ Tránsito y Movimientos Migratorios ☐ Académicos ☐ Procedimientos Administrativos o Judiciales ☐ Patrimoniale ☐ Salud ☐ Ideológicos ☐ De origen ☐ Características Personales ☐ Vida Sexual

Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área

ANEXO 2

FORMATO B

Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	Haga clic aquí para escribir una fecha.
NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN	
CARGO	
AREA	
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	Haga clic aquí para escribir una fecha.
FUNDAMENTO LEGAL PARA OBTENCIÓN DE LOS DATOS PERSONALES.	
RESGUARDO DE LOS SOPORTES	
USUARIOS	
MEDIDAS DE SEGURIDAD FISICAS TÉCNICAS Y ADMINISTRATIVAS APLICADAS	
LAS CAUSAS ENUNCIADAS EN EL FORMATO A	
LO QUE EL TITULAR DEL ÁREA CONSIDERE PERTINENTE	
APARTADO B	
ADMINISTRADOR DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
USUARIOS DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
LOS HECHOS DE MODO TIEMPO Y LUGAR ENUNCIADOS EN EL FORMATO A	
RESGUARDANTE SOPORTE FÍSICO O ELECTRÓNICO VULNERADO	