



INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA  
Y PROTECCIÓN DE DATOS PERSONALES  
DEL ESTADO DE JALISCO

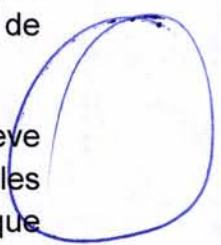
# GUÍA PARA ELABORAR UN DOCUMENTO DE SEGURIDAD

Formato guía para sujetos obligados

El presente documento tiene como objeto ser una guía de apoyo para los sujetos obligados en la realización de su documento de seguridad, como parte del acompañamiento del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, en el cumplimiento a las disposiciones del artículo 35, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

A lo largo de la guía se señala como atender a cada una de las diecinueve fracciones de los artículos 35 y 36, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios que corresponden al contenido del documento de seguridad.

Es importante aclarar que se trata de una guía de acompañamiento para los sujetos obligados, y no un formato obligatorio, ya que los responsables del tratamiento de los datos personales, pueden utilizar cualquier estilo o formato, siempre y cuando atiendan a cabalidad con las disposiciones de Ley.



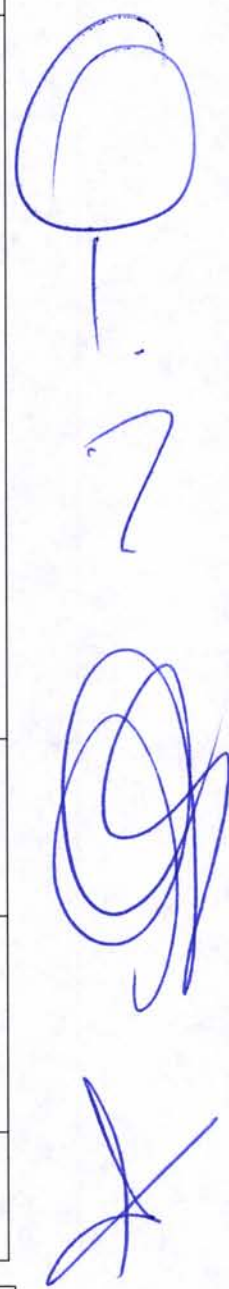
# Documento de Seguridad

## Contenido

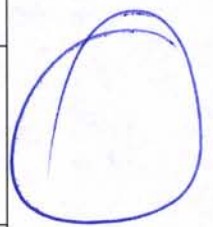
Glosario .....	3
Medidas de seguridad implementadas.....	6
Procedimientos de respaldo y recuperación de datos personales.....	8
Controles y mecanismos de seguridad para las transferencias.....	8
Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales.....	10
Controles de Identificación y Autenticación de Usuarios.....	10
Técnicas de Supresión y Borrado Seguro de Datos Personales .....	11
Análisis de riesgos .....	12
Identificación de Medidas de Seguridad.....	12
Gestión de vulneraciones.....	22
Plan de respuesta .....	22
Mecanismos de monitoreo y revisión de las medidas de seguridad.....	24
Análisis de brecha.....	25
Plan de trabajo .....	26
Programa General de Capacitación.....	27
Plan de Contingencia.....	27
Catálogo de Sistemas de Tratamiento de Datos Personales .....	27
Bibliografía .....	30

# Glosario

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.
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.
DMZ	En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de <i>demilitarized zone</i> ) o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos ( <i>hosts</i> ) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos ( <i>hosts</i> ) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos ( <i>host</i> ) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.
DNS	Un Servidor DNS en informática responde a las siglas <i>Domain Name System</i> . Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada.
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.
Evaluación de impacto en la protección de datos personales	Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto	Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
LAN	Una red de área local o LAN (por las siglas en inglés de <i>Local Area Network</i> ) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley General de Transparencia	Ley General de Transparencia y Acceso a la Información Pública.
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.



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.
N/A	No aplica.
Responsable	Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios 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 son 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.

# Medidas de seguridad implementadas

(Pública I. F., 2009)

Es importante aclarar las diferencias que existen entre las medidas de seguridad administrativa, física y técnica para que se cuente con los elementos teóricos al momento de elaborar el Documento de Seguridad.

a) Las medidas de seguridad **administrativa** son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

- Política de seguridad. Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.
- Cumplimiento de la normatividad. Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable.
- Organización de la seguridad de la información. Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.
- Clasificación y control de activos. Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.
- Seguridad relacionada a los recursos humanos. Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.
- Administración de incidentes. Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.
- Continuidad de las operaciones. Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

b) Las medidas de seguridad **física** atañen a las acciones que deben implementarse para contar con:

- Seguridad física y ambiental. Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

c) Las medidas de seguridad **técnica** son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

- Gestión de comunicaciones y operaciones. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

- Control de acceso. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

- Adquisición, desarrollo, uso y mantenimiento de sistemas de información. Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

- Tipo de soportes: físicos y electrónicos. Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales están estrechamente relacionadas con el tipo de soportes utilizados. Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el INAI:

- **Soportes físicos.** Son los medios de almacenamiento inteligibles 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 otros.
- **Soportes 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, vídeo 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 Decimoséptimo y el Trigésimo de los Lineamientos hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos —físicos o electrónicos— en los cuales residen los datos personales del sistema que custodia el sujeto obligado. Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en:

- i) Soporte físico;
- ii) Soporte electrónico; o
- iii) Ambos tipos de soportes.

## **Procedimientos de respaldo y recuperación de datos personales**

(Pública I. F., 2009)

Es el procedimiento que se implementa cuando queremos tener resguardados nuestros datos o documentos en caso de que suceda algún imprevisto con nuestros sistemas informáticos, más precisamente con los discos duros, ya que estos son bastante delicados y son uno de los componentes informáticos con más alta probabilidad de presentar fallos.

Un respaldo de información bien organizado y estructurado nos permitiría volver a acceder a nuestros documentos para continuar trabajando con la mayor velocidad y eficiencia posibles, además de evitar que información importante se pierda, y con ella años de trabajo.

Los procedimientos de respaldo y recuperación desarrollados deben formar parte de un plan de respaldo y recuperación, el cual debe ser documentado y comunicado a todas las personas involucradas. Dado que, a lo largo del tiempo, varias características que se consideran para desarrollar este plan sufren cambios (software utilizado, soporte, etc.), el plan debe ser revisado, y de ser necesario modificado de manera periódica. El plan debe contener todos los ítems detallados a continuación y cualquier otro que mejore la realización del trabajo o clarifique la tarea.

## **Controles y mecanismos de seguridad para las transferencias**

(Pública I. F., 2009)

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, exceptuando las realizadas entre responsables en cumplimiento de una disposición legal o en el ejercicio de sus atribuciones, así mismo en el ámbito internacional cuando se encuentren previstas en una ley o tratado suscrito y ratificado por México, o sea solicitada por una autoridad u organismo internacional competente.

### **Transferencias mediante el traslado de soportes físicos**

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.

### **Transferencias mediante el traslado físico de soportes electrónicos**

En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en 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. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

Al realizar transferencias físicas de soportes electrónicos se deberá considerar lo dispuesto en los ordenamientos aplicables, como lo son: Los oficios de comisión para el personal autorizado y asegurar que la entrega sea a los titulares de la información o a personal autorizado para recibirla, los medios para garantizar la confidencialidad de la información, utilizar las leyendas de clasificación, registro en bitácoras de transferencia, cifrar la información, utilizar contraseñas etc...

### **Transferencias mediante el traslado sobre redes electrónicas**

En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

## Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales

<p><b>Bitácoras de Acceso</b></p>	<p>1. Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:</p> <ul style="list-style-type: none"> <li>• Nombre y cargo de quien accede</li> <li>• Identificación del Expediente</li> <li>• Fojas del Expediente</li> <li>• Propósito del Acceso</li> <li>• Fecha de Acceso</li> <li>• Hora de Acceso</li> <li>• Fecha de Devolución</li> <li>• Hora de Devolución</li> </ul> <p>2. Las bitácoras se encuentran en soporte físico</p> <p>3. Son resguardadas por los coordinadores de cada área en el lugar que para tal efecto designen, el cual, debe estar resguardado bajo llave.</p>	<p>Se deben enumerar los datos que contendrán dichas bitácoras</p> <p>El tipo de soporte de las bitácoras, físico o electrónico</p> <p>Se señala quien tiene el resguardo de las bitácoras y las características del mismo</p>
<p><b>Vulneraciones a la Seguridad de los Datos Personales</b></p>	<p>La bitácora de vulneraciones contiene la siguiente información</p> <ol style="list-style-type: none"> <li>1. Nombre de quien reporta el incidente</li> <li>2. Cargo</li> <li>3. La fecha en la que ocurrió;</li> <li>4. El motivo de la vulneración de seguridad; y</li> <li>5. Las acciones correctivas implementadas de forma inmediata y definitiva.</li> </ol>	<p>Enumerar los datos que contendrán las bitácoras de vulneraciones</p>

## Controles de Identificación y Autenticación de Usuarios

Se debe señalar y detallar la forma en que se identifica al personal del sujeto obligado, así como la forma en que se autentifica a cada uno. Por ejemplo:

1. Los empleados de la Secretaría deben portar en todo momento su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre
- Cargo

Al reverso:

- Vigencia
- Número de Empleado
- Firma del Titular de la Institución
- Sitio Oficial
- RFC
- Domicilio de la Institución
- Teléfono de la Institución

2. En el ambiente electrónico todas las computadoras precisan de un nombre de usuario y contraseña para ingresar.

También se debe señalar y detallar la forma en que se identifica y registra a toda persona que ingresa a las instalaciones, por ejemplo:

- A los ciudadanos se les solicita identificación oficial con fotografía, únicamente cuando es necesario que acrediten su identidad ante el sujeto obligado.

## Técnicas de Supresión y Borrado Seguro de Datos Personales

(Ciberseguridad)

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobreescritura en la totalidad del área de almacenamiento de la información.

### 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 de 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 específicas 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 son regrabables, como los CD y DVD.

## **Análisis de riesgos**

(Pública I. F., 2014)

Los Lineamientos Generales de Protección de Datos Personales para el Sector Público establecen los puntos a considerar para realizar el análisis de riesgo contenido en el Documento de Seguridad. Se debe de tomar en cuenta el valor de los datos personales el cual depende de la clasificación de los mismos y su ciclo de vida. Por otro lado, el valor de los datos personales que forman parte del tratamiento y la exposición de los mismos deben de ser considerados al realizar dicho análisis. A lo anterior se le deben de sumar las consecuencias negativas para los titulares en caso de alguna vulneración y finalmente los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.

Por lo tanto, en aras de las mejores prácticas, la Metodología BAA (Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante) publicada en marzo del 2014 por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (antes IFAI), ha sido integrada en parte para que el responsable pueda entender mejor lo que se refiere al análisis de riesgo, para más información se recomienda que se consulte la metodología.

### **Análisis de Riesgos conforme a la Metodología BAA**

(Pública I. F., 2014)

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad. Esta

metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales (Figura 1):

- **Beneficio**, factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad**, factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.
- **Anonimidad**, factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos. Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles. En la siguiente imagen se ilustra el procedimiento de obtención del valor de riesgo latente para los particulares:

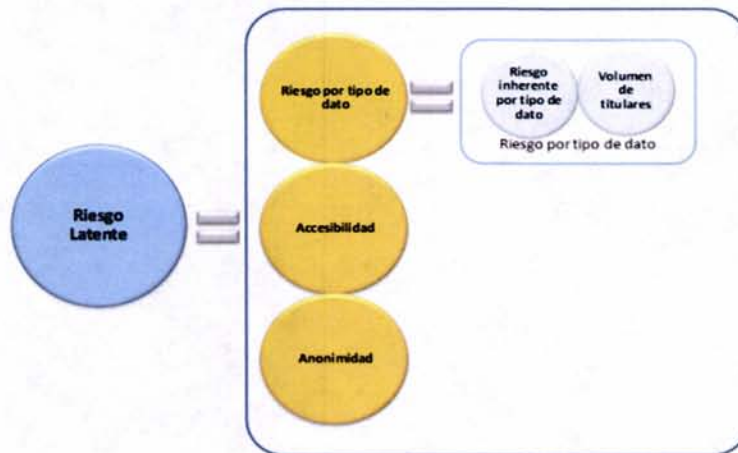


Figura 1. Cálculo de riesgo latente

El nivel de riesgo por tipo de dato es igual al beneficio que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

1. Tener el nivel de riesgo inherente de cada tipo de dato que se trate, y;
2. Calcular el volumen de titulares, cuantificando el número de personas de las que se traten datos personales.



Figura 2. Identificación de riesgo por tipo de dato

El nivel de riesgo inherente de cada tipo de dato se determina de acuerdo a la sección 2. Identificación y clasificación de datos personales. Mientras que el volumen de titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

- <500: Datos de hasta 500 personas
- <5k: Datos entre 501 hasta 5,000 personas
- <50k: Datos entre 5,001 hasta 50,000 personas
- <500k: Datos entre 50,001 hasta 500,000 personas
- >500k: Datos de más de 500,000 personas



Es importante que para llevar a cabo la cuantificación de titulares se considere tanto los soportes físicos, como los electrónicos. Se debe seleccionar uno de los rangos anteriores según el tipo de dato y su nivel de riesgo inherente, por ejemplo:

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares
Patrimoniales	Medio	<50k

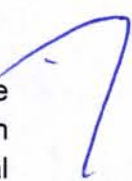
Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de riesgo por tipo de dato que se trata en la organización. Se han establecido cinco niveles posibles (Figura 3) nombrados con valor numérico del 1 al 5, tal como se muestra en la siguiente imagen, donde 1 es el nivel más bajo y 5 el más alto:

TIPO DE DATO	RIESGO INHERENTE	<500	<5k	<50k	<500k	>500k
<ul style="list-style-type: none"> <li>* Información adicional de tarjeta bancaria</li> <li>* Titulares de alto riesgo</li> </ul>	Reforzado R	4	4	5	5	5
<ul style="list-style-type: none"> <li>* Salud</li> <li>* Origen, creencias e ideológicos</li> </ul>	Alto C	1	2	3	3	3
<ul style="list-style-type: none"> <li>* Ubicación</li> <li>* Patrimoniales</li> <li>* Autenticación</li> </ul>	Medio B	1	1	2	3	3
<ul style="list-style-type: none"> <li>* Jurídicos</li> <li>* Tarjeta Bancaria</li> </ul>						
<ul style="list-style-type: none"> <li>* Personales de identificación</li> </ul>	Bajo A	1	1	1	1	1

Figura 3. Nivel de riesgo por tipo de dato

A continuación se detallan los niveles mencionados:

Riesgo por tipo de dato Nivel 1, ocurre cuando:



- El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

Riesgo por tipo de dato Nivel 2, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas
- El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas

Riesgo por tipo de dato Nivel 3, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante
- El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante

Riesgo por tipo de dato Nivel 4, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas

Riesgo por tipo de dato Nivel 5, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

En la Tabla 2 se muestra una relación del tipo de datos con el nivel de riesgo correspondiente.

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1

Tabla 2. Nivel de riesgo por tipo de dato

Este nivel de riesgo servirá para determinar los controles que debe considerar el responsable para la protección de datos personales, que se describen en la sección relativa a la identificación de medidas de seguridad.



*\*Para mayor información, consultar la Metodología de Análisis de Riesgo BAA del Instituto Federal de Acceso a la Información Pública.*

## Identificación de Medidas de Seguridad

<b>Medidas de Seguridad Administrativas</b>	<b>Control</b>	<b>Parámetro (Llenar con la forma en que se va a implementar o ya se implementó)</b>
	Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	
	Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	
	Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	
	Atender las necesidades de seguridad cuando se trata con ciudadanos: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los ciudadanos, a los activos o información de la organización.	
	Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	
	Inventario de activos: Todos los activos deben ser claramente identificados y —se debe	

	elaborar y mantener un inventario de los activos más importantes.	
	Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	
	Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	
	Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo, debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	
	Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	
	Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	
	Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	
	Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	
	Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	
	Procedimientos y responsabilidades de	

	<p>respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad</p>	
	<p>Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.</p>	
	<p>Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.</p>	
	<p>Retorno de los activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.</p>	
<p><b>Medidas de Seguridad Avanzadas para Accesos desde Red Interna RI-3 conforme a la metodología BAA del INAI</b></p>	<p><b>Control</b></p>	<p><b>Parámetro</b></p>
	<p>Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación</p>	
	<p>Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.</p>	
	<p>Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.</p>	
	<p>Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información</p>	

	en tránsito.	
	Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	
	Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	
	Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	
	Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	
	Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	
	Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	
	Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	
	Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	
<b>Medidas de Seguridad Físicas</b>	<b>Control</b>	<b>Parámetro</b>
	Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento	

	de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	
	Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	
	Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	
	Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	
<b>Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad</b>	<b>Control</b>	<b>Parámetro</b>
	Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	
	Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	
	Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	
	Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	
	Administración de privilegios: Deberá	

	restringirse y controlarse la asignación y uso de privilegios.	
	Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	
	Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	
	Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	
	Fuga de información: Se deben prevenir las oportunidades de fuga de información.	
	Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	
	Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	
	Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	
	Definir e implementar listas de control de acceso (ACL)	
	Controles de DNS	
	Únicamente permitir servicios públicos dentro de la DMZ	
	Mejores prácticas de configuración del FW	
	Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa	
	Red de terceros conectada a la zona desmilitarizada (DMZ) externa	

	Controles de tráfico entrante y saliente	
	Implementar y monitorear sistemas de prevención de Intrusos (IPS)	

## Gestión de vulneraciones

### Plan de respuesta

(Instituto Nacional de Transparencia, 2018)

La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Por lo tanto, elaborar un plan de respuesta a incidentes es probablemente una de las tareas más complejas en seguridad de la información. Por lo anterior, en este apartado se ofrecerán recomendaciones para atender incidentes de seguridad, a fin de prevenir y mitigar las vulneraciones a la seguridad de los datos personales. Para ello se desarrollará (i) la relación entre las alertas y los incidentes de seguridad, (ii) las características particulares de un incidente de seguridad cuando involucra datos personales y; (iii) las etapas del plan de respuesta a incidentes de seguridad.

Antes de iniciar con la descripción del proceso de respuesta a incidentes de seguridad, es necesario abordar una serie de conceptos base interrelacionados que son activo, riesgo, alerta, incidente, vulneración y revelación. Como se señaló en las definiciones, un activo es todo elemento de valor para una organización, involucrado en el tratamiento de datos personales, por ejemplo, la base de datos de empleados, el registro de acceso a un edificio, los equipos de cómputo de una oficina, el correo electrónico o el almacenamiento de información en la nube. Estos activos son susceptibles a amenazas, es decir, a factores externos que tienen el potencial de dañarlos, por ejemplo, una descarga eléctrica puede dañar un equipo de cómputo, o un empleado podría acceder a información sin que esté autorizado para ello.

Para que una amenaza tenga efecto, requiere explotar una vulnerabilidad, debilidad o falla propia de un activo, por ejemplo, la descarga eléctrica sólo puede afectar a los equipos de cómputo que no tenga un regulador de voltaje. Por otro lado, el empleado podría acceder sin autorización a una base de datos si no está protegida con contraseña.

Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos<sup>6</sup> (Figura 2). Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.



Figura 2. Estructura de un riesgo

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento. Sin embargo, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte.

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:

Ejemplos de alertas 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 medios de 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 del hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento.
Software malicioso <sup>7</sup>	Diferentes categorías de software malicioso (malware) como virus, troyanos, software de acceso y control remoto (RAT, 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. Escaneo de redes, utilización de puertas traseras en el software, intentos de acceso no autorizado, inferencia de contraseñas, ataques de denegación de servicio.
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.

Tabla 2. Ejemplos de incidentes de seguridad

El plan de respuesta a incidentes se enfoca en la mejora continua, a través de estándares internacionales en la materia y de innovaciones tecnológicas.

*\*Para más información, consultar las recomendaciones para el manejo de incidentes de seguridad de datos personales del INAI en la página*

*[http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones\\_Manejo\\_IS\\_DP.pdf](http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf)*

## Mecanismos de monitoreo y revisión de las medidas de seguridad

En este apartado se debe de señalar las acciones que se tomarán para mantener actualizadas las medidas de seguridad, describiendo la forma en que se llevarán a cabo y la temporalidad que tendrán.

# Análisis de brecha

(ProtektNet)

La realización de un análisis de brecha va enfocado a la seguridad de los datos personales recabados, realizando un diagnóstico de las prácticas de seguridad de la información con las que cuenta en ese momento el sujeto obligado y las que deberían de tenerse en base a las mejores prácticas.

Las mejores prácticas deben de cubrir las áreas o dominios de la seguridad de la información, para que permita evaluar de manera amplia para identificar las practicas que se deberán de llevar a cabo para un mayor cumplimiento de las obligaciones en materia de protección de datos personales, para de esta manera establecer el nivel de madurez de las prácticas realizadas por el sujeto obligado y posteriormente definir las acciones que se llevarán a cabo para disminuir la brecha entre la situación actual y las mejores prácticas.

Algunos de los aspectos a evaluar y ponderar para tener una visión más completa y concreta sobre el estado actual de la seguridad de los datos personales y los aspectos existentes son:

- **Seguridad institucional.**  
Control de la información compartida con terceros
- **Activos del responsable**  
Asignación de responsabilidades y clasificación
- **Seguridad en recursos humanos**  
Cuidar la seguridad de los recursos humanos previo a la contratación, durante y una vez que haya culminado su trabajo.
- **Seguridad física y ambiental**  
Áreas seguras y protección de equipamiento
- **Operación, procedimientos y comunicación**
- **Cumplimiento con leyes y lineamientos**
- **Control de acceso a la información**  
Derechos y control de acceso a aplicaciones, redes y sistemas operativos  
Protección móvil y trabajo remoto
- **Seguridad de sistemas de información**  
Procesos de información  
Controles criptográficos  
Protección de archivos de sistema
- **Incidentes de seguridad de información**

# Plan de trabajo

Elija un elemento.

Haga clic aquí para escribir texto.

Haga clic aquí para escribir texto.

Conforme a los elementos faltantes encontrados en el análisis de brecha, se deben de implementar en el Plan de Trabajo, señalando el parámetro y el control

Haga clic aquí para escribir texto.

Control (Medida de seguridad faltante o actividad a realizar)	Parámetro (Qué es lo que se debe hacer)
Ejemplo: Fuga de información: Se deben prevenir las oportunidades de fuga de información.	
Ejemplo: Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	
Ejemplo: Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ejemplo: Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo

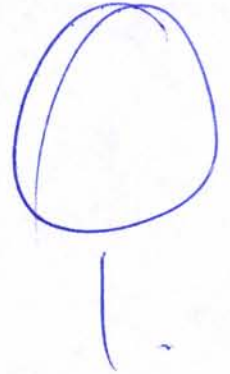
Haga clic aquí para escribir texto.

Control (Medida de seguridad faltante o actividad a realizar)	Parámetro (Qué es lo que se debe hacer)




Haga clic aquí para escribir texto.

Control (Medida de seguridad faltante o actividad a realizar)	Parámetro (Qué es lo que se debe hacer)



## 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.



## Plan de Contingencia

Elaborar un Plan de Contingencia respecto a la seguridad y protección de los datos personales, en caso de vulneraciones



## Catálogo de Sistemas de Tratamiento de Datos Personales

Sistema de tratamiento de los pagos a empleados



<b>Administrador</b>	<b>Nombre de la persona a cargo</b>	<b>Bases de datos</b>	<b>Enumerar las bases de datos personales que formen parte del sistema</b>
<b>Cargo:</b>	<b>El cargo que ostenta la persona</b>		
<b>Área</b>	<b>Área de adscripción</b>		
<b>Funciones y obligaciones</b>	<b>Enumerar las funciones y obligaciones de la persona de acuerdo a su puesto.</b>		
<b>Personal autorizado para tratamiento (Incluir a las personas que formar parte del sistema al tratar datos personales)</b>			
<b>Nombre del puesto</b>	<b>Nombre de la persona</b>	<b>Bases de datos</b>	<b>Enumerar las bases de datos personales que formen parte del sistema</b>
<b>Funciones y obligaciones:</b>	<b>Enumerar las funciones y obligaciones de la persona de acuerdo a su puesto.</b>		
<b>Nombre del puesto</b>	<b>Nombre de la persona</b>	<b>Bases de datos</b>	<b>Enumerar las bases de datos personales que formen parte del sistema</b>
<b>Funciones y obligaciones:</b>	<b>Enumerar las funciones y obligaciones de la persona de acuerdo a su puesto.</b>		
<b>Tipo de datos personales pertenecientes al sistema de tratamiento de los pagos a empleados</b>			
<b>Inventario:</b>	<b>Enlistar los datos personales que se recaban en dicho sistema.</b>		
<b>Bases de datos</b>	<b>Enlistar todas las bases de datos tratadas en el sistema.</b>		
<b>No. De titulares</b>	<b>De cuantas personas se tienen recabados datos personales en el sistema.</b>		
<b>Controles de seguridad para las bases de datos</b>	<b>Las formas en las que se protegen las bases de datos para evitar un acceso no autorizado.</b>		
<b>Estructura y descripción del Sistema de tratamiento</b>			
<b>Tipo de soporte:</b>	<b>Los tipos de soporte en el sistema de tratamiento</b>		

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.	
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales</b>		
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.	
<b>Las bitácoras de acceso y- operación cotidiana</b>		
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.	
<b>Las bitácoras de vulneraciones de seguridad</b>		
ID	Soporte	Responsable
Clave de la bitácora	Físico o Electrónico	Administrador del sistema

## Bibliografía

Ciberseguridad, I. N. (s.f.). *Guía sobre borrado seguro de la información*. Recuperado el 13 de 07 de 2018, de [https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_ciberseguridad\\_borrado\\_seguro\\_metad.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf)

Instituto Nacional de Transparencia, A. a. (Junio de 2018). *Instituto Nacional de Transparencia, Acceso a la Información*. Recuperado el 03 de 08 de 18, de Recomendaciones para el manejo de incidentes de seguridad de datos personales: [http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones\\_Manejo\\_IS\\_DP.pdf](http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf)

ProtektNet. (s.f.). Recuperado el 02 de 08 de 2018, de <https://protektnet.com/servicios/cumplimiento-normativo/analisis-de-brecha-de-seguridad-de-la-informacion/>

Pública, I. F. (19 de 07 de 2009). *Guía para la elaboración de un Documento de seguridad v1.4*. Recuperado el 13 de 07 de 2018, de [https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia\\_elaboracion\\_Documento\\_seguridad.pdf](https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia_elaboracion_Documento_seguridad.pdf)

Pública, I. F. (Marzo de 2014). *Son tus datos*. Recuperado el 13 de Julio de 2018, de [https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA\\_2014.pdf](https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA_2014.pdf)



**Cynthia Patricia Cantero Pacheco**

Presidenta del Pleno



**Salvador Romero Espinosa**

Comisionado Ciudadano



**Pedro Antonio Rosas Hernández**

Comisionado Ciudadano



**Miguel Ángel Hernández Velázquez**

Secretario Ejecutivo

----- La presente hoja de firmas, forma parte integral de la « *Guía para Elaborar un Documento de Seguridad* ».» aprobado en la Vigésimo Octava Sesión Ordinaria del Pleno del Instituto, celebrada en fecha 22 Veintidós de Agosto del año 2018 dos mil dieciocho. -----