Guía para la Elaboración de un Documento de Seguridad

¿Qué es un Documento de Seguridad?

Es el documento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas requeridas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Lo genera el responsable de los sistemas de datos personales.

¿Cuál es el objeto del Documento de Seguridad?

Garantizar que los programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con las medidas de seguridad para la protección de datos personales y las obligaciones previstas en la Ley de Datos.

¿Qué se busca al generar el documento de seguridad?

Que cualquier medio que se utilice para el tratamiento de datos personales en los Sistemas de Datos institucionales, se cuente con las medidas de seguridad que garanticen su protección.

¿Cuál es la finalidad del Documento de Seguridad?

Que el Sujeto Obligado cumpla con el tratamiento lícito, seguro y responsable de los datos personales, además:

- Identificar el universo de sistemas de datos personales que posee cada dependencia o entidad
- Clasificar el tipo de datos personales que contiene cada uno.
- Designar a los responsables, encargados, usuarios de cada sistema.
- Establecer las medidas de seguridad concretas implementadas.

¿Para qué sirve un Documento de Seguridad?

- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
- Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales; así como poner en práctica un programa de capacitación y actualización del personal.

- Fijar parámetros para la actuación de los responsables.
- Crear políticas institucionales para la Protección de los Datos Personales.

¿En qué momento se debe informar al titular, la existencia de un Sistema de Datos Personales mediante el cual serán tratados y protegidos sus Datos Personales?

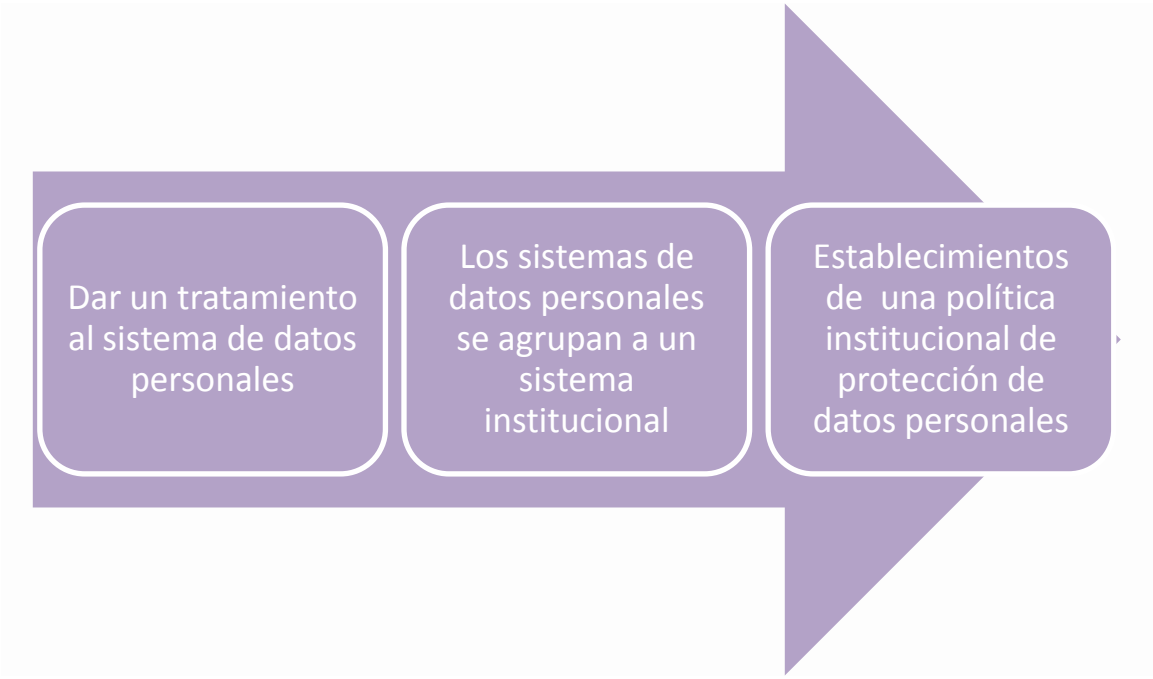
Cuando acude ante el responsable para realizar un trámite o gestionar un servicio y éste pone a su disposición el Aviso de Privacidad, el cual contiene entre otras cosas el Nombre del Sistema de Datos Personales, las categorías de datos que se recaban y el ciclo de vida del tratamiento de los mismos.

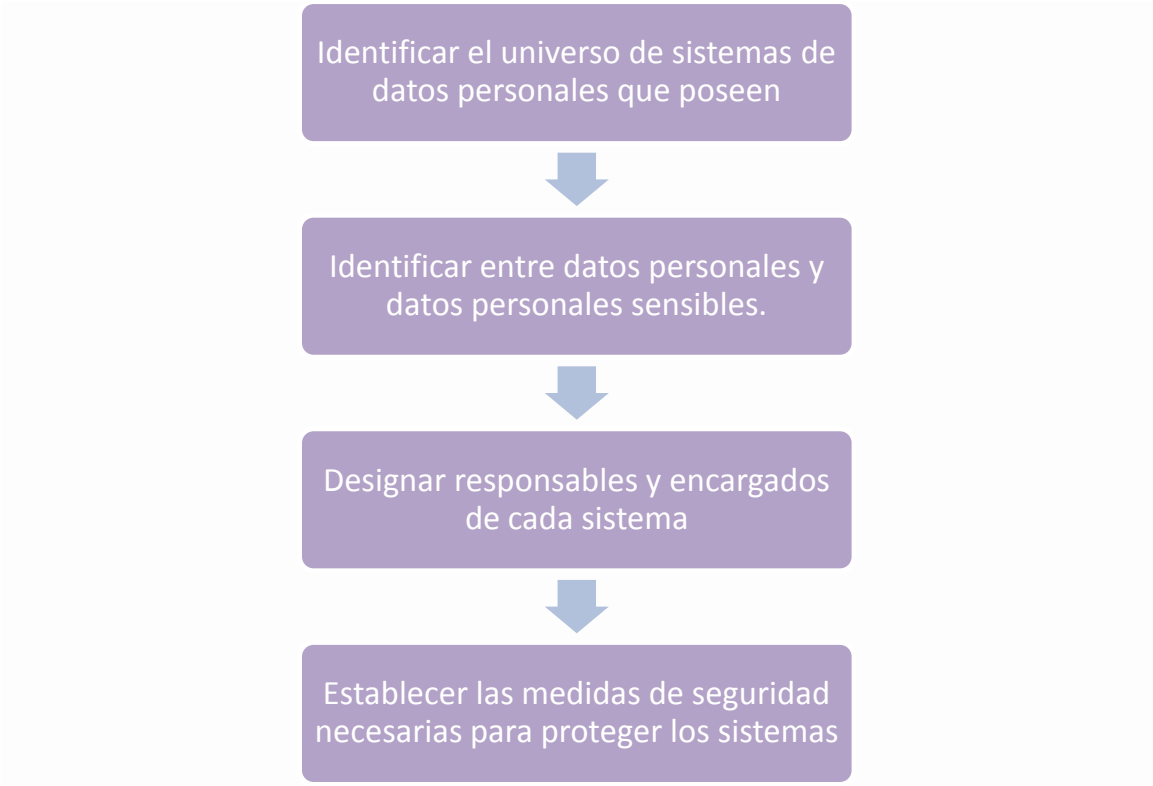
¿En qué consiste el Inventario de datos personales?

Enlistar el tipo y categorías de los datos personales y en su caso los datos personales sensibles recabados.

El inventario de datos personales se refiere a qué datos personales se tienen, tipo de datos (sensibles o no), cuántos sistemas de datos se tienen y en qué soportes se tiene la información, si es un documento físico o se encuentra en formato electrónico.

¿Cuáles son los pasos para la elaboración de un Documento de Seguridad?





¿Cuáles son las funciones y obligaciones de los usuarios y encargados, personas que intervienen en el tratamiento de datos personales, en el caso de que los hubiera?

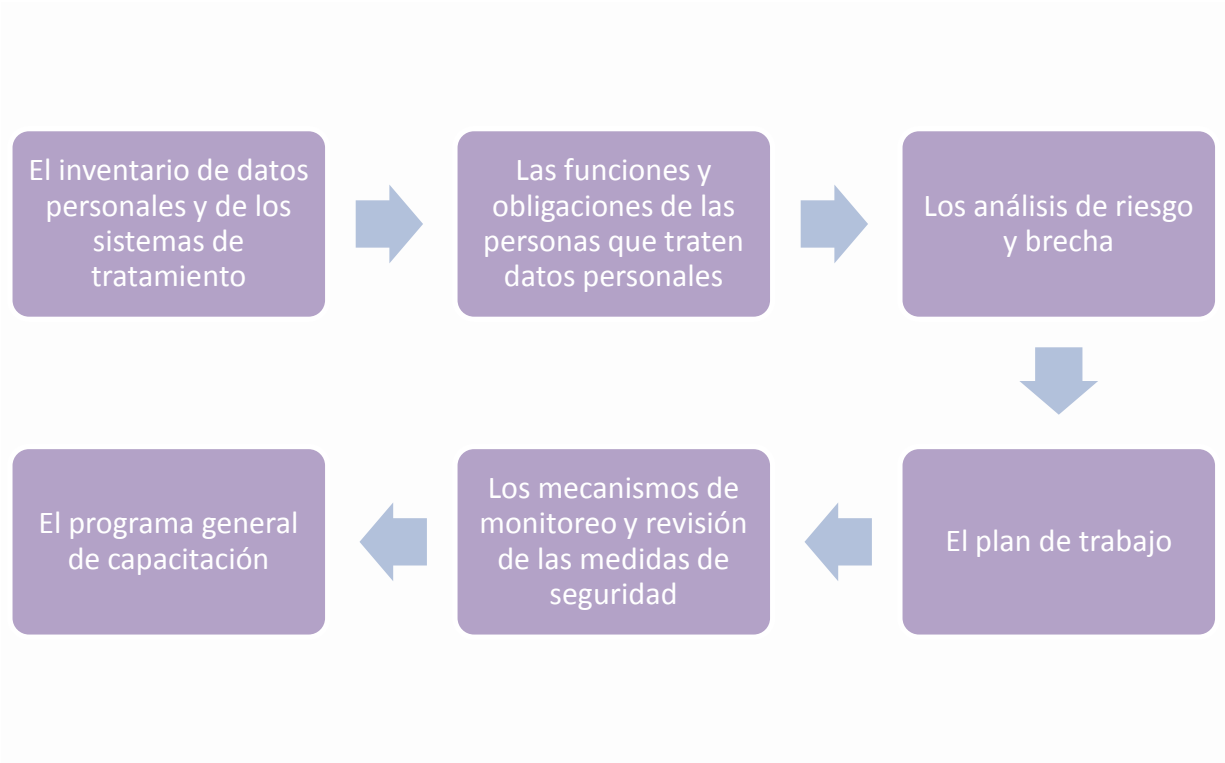
Responsable.- Es quien se encarga de elaborar políticas y programas, poner en práctica un programa de capacitación actualización sobre las obligaciones y deberes, revisar periódicamente las políticas y programas de seguridad de datos personales, determinar las modificaciones que se requieran, establecer un sistema de supervisión de vigilancia interna y externa, auditorias, adoptar las medida de seguridad necesarias, elaborar los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, registrar ante el instituto los sistemas de datos personales, las modificaciones o supresiones de los mismos, coordinar y supervisar la adopción de medidas de seguridad a que se encuentran sometidos los sistemas de datos.

Usuario.- Deberá identificar, clasificar, borrar, prevenir el acceso no autorizado, a las instalaciones físicas, aéreas críticas, prevenir daños e interferencias a sus instalaciones, proteger los recursos móviles, portátiles, soportes físicos, electrónicos, dar mantenimiento al sistema, asegurar la disponibilidad e integridad, proteger el entorno digital, prevenir el acceso a las bases de datos, a la información, los recursos, generar esquemas de privilegios, revisar la configuración de seguridad, apoyar en la adquisición, operación, desarrollo, y mantenimiento del software y hardware, gestionar las comunicaciones,

operaciones y medios de almacenamiento de la información en el tratamiento de datos personales.

Encargado.- Lleva a cabo el tratamiento de los datos personales conforme a las instrucciones del responsable, abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable, implementar las medidas de seguridad conforme a la naturaleza de los datos, informar al responsable cuando ocurra una vulneración, guardar la confidencialidad, suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

¿Cuáles son los elementos indispensables del Documento de Seguridad?



¿Qué es el registro de incidencias?

Es el registro de vulneraciones a la seguridad del sistema, consistente en la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación de la información.

¿Qué tiene que hacer el responsable en caso de que ocurran incidencias?

Deberá analizar las causas por la cuales se presentó la incidencia, con acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los

datos personales, con el fin de que la vulneración no se repita, e informar al titular de los datos y al órgano garante para tomar las medidas de mitigación correspondientes.

¿De qué manera se llevará el registro de las incidencias?

Mediante una bitácora de vulneraciones, en donde se anotará nombre y cargo de quien reporta el incidente, el número de vulneraciones, describirá la misma, la fecha en que ocurrió, el motivo de ésta y las acciones implementadas de forma inmediata y definitiva.

¿Qué obligación tendrá el responsable en caso de una vulneración?

Deberá informar sin dilación alguna al titular y al Instituto (INFO) en cuanto confirme que ocurrió la vulneración.

¿Qué es lo que debe de informar al titular de los datos personales?

Por lo menos debe de informar la naturaleza del incidente, los datos personales comprometidos, los derechos del titular que puede adoptar para proteger sus datos, las acciones correctivas que realizó en forma inmediata y los medios en donde puede obtener más información.

¿Qué es lo que debe de informar al Instituto una vez que ocurrió la vulneración?

Las medidas de mitigación llevadas a cabo, los niveles de seguridad que tiene adoptados y el documento de gestión en donde el Instituto realizará las recomendaciones y medidas pertinentes para la protección de los datos personales.

¿Qué tendrá que hacer el Instituto al momento de ser informado de una incidencia?

Realizará una inspección o verificación sobre las medidas adoptadas para mitigar el impacto, emitir las recomendaciones para que sean solventadas en el término que establezca el Instituto.

¿Qué es la identificación y la autenticación?

Identificación.- Persona autorizada (Encargado y/o Usuario) por el responsable para que acceda a su sistema.

Autenticación.- El Sistema reconoce a la persona (Encargado y/o Usuario) que accede o utiliza el sistema.

¿En qué consiste el Control de acceso, gestión de soportes y copias de respaldo y recuperación?

Control de acceso.- Registro detallado de accesos a un sistema automatizado que permite de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad.

Gestión de Soportes.- Garantizar la correcta conservación de los documentos, la localización y consulta de la información por el personal autorizado en el documento de seguridad, el cual debe de almacenar datos o documentos, u objeto susceptible de ser tratado en un sistema de información y se puedan grabar y recuperar datos en pendrive, discos duros externos, CD'S, DVD'S, memorias USB, scanner, inventariar, registrar las salidas y entradas de información aún de los correos electrónicos, el traslado de información, cifrado de datos, generar contraseñas y usuarios.

¿Qué es una copia de respaldo?

Refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo, catástrofe, desastre y que es fundamental para la recuperación de la información.

¿Qué es la recuperación de datos?

Conjunto de técnicas y procedimientos utilizados para acceder y extraer la información almacenada en medios de almacenamiento digital que por daño o avería no pueden ser accesibles de manera usual ya sea por falla en el equipo, catástrofe o desastre natural.

¿En qué reside el análisis de riesgo?

Son los proyectos e iniciativas de mejoras de la seguridad de información, en la que se debe de considerar las amenazas, vulneraciones y los recursos involucrados en su tratamiento.

¿Qué es el análisis de brecha?

Es el estudio comparativo de las medidas de seguridad existentes contra las medidas de seguridad faltantes; es decir donde estamos ahora y donde queremos estar (estado actual y el objetivo a alcanzar o que tenemos ahora y que nos hace falta).

¿Quién es el Responsable de seguridad?

Es la persona designada por el Sujeto Obligado para establecer y mantener las medidas de seguridad para la protección de datos personales de sus sistemas.

¿Cuáles serán las actividades del responsable de seguridad?

Crear políticas internas para la gestión y tratamiento de los datos personales, el ciclo de vida de los Datos Personales (obtención, uso y supresión), definir las funciones y obligaciones del personal involucrado, elaborar el inventario de Datos Personales, realizar el análisis de riesgo considerando las amenazas y vulnerabilidades existentes, solicitar los recursos involucrados en su tratamiento para la compra de hardware, software, contratación de personal del responsable, realizar el análisis de brecha, elaborar un plan de trabajo, implementar las medidas de seguridad faltantes, las políticas de gestión y tratamiento, monitorear y revisar de manera periódica las medidas de seguridad

implementadas, las amenazas y vulneraciones, diseñar y aplicar capacitaciones del personal bajo su mando, dependiendo de sus roles y responsabilidades.

¿Qué es el registro de acceso?

Constancia de ingresos al sistema mediante la identificación, autenticación y autorización, constancia de acceso no autorizado, constancia de seguridad en la conexión, constancia de eventos y actividades llevadas a cabo por los usuarios.

¿Qué es el registro de telecomunicaciones?

Constancia de envío, recepción o almacenamiento de mensajería, aplicaciones que contienen datos personales.

¿En qué consiste el mecanismo de monitoreo?

Es el Control del desarrollo cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo y como resultado de un proceso de mejora continua.

¿En qué consiste la revisión de las medidas de seguridad?

Es la implementación de acciones correctivas y preventivas periódicas ante una vulneración a la seguridad.

¿Qué es el plan de trabajo?

Es la herramienta con la que se organiza y simplifica las actividades necesarias para la implementación de medidas de seguridad faltantes para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

¿En qué consiste programa general de trabajo?

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

ESTRUCTURA DEL DOCUMENTO DE SEGURIDAD

La estructura para elaborar el Documento de Seguridad lo podrás encontrar en el Manual de Procedimientos de la Unidad de Transparencia del Instituto Electoral de la Ciudad de México (Anexo 5).

Documento de Seguridad	**Inventario de datos personales en los sistemas de datos**
	Funciones y obligaciones de las personas que intervienen en el tratamiento de datos personales, usuarios y encargados
	Registro de incidencias
	Identificación y autenticación
	Control de acceso, gestión de soportes, y copias de respaldo y recuperación
	Análisis de riesgo
	Análisis de brecha
	Responsable de seguridad
	Registro de acceso y telecomunicaciones
	Mecanismos de monitoreo y revisión de las medidas de seguridad
	Plan de trabajo
	Programa general de capacitación

FORMATO DE DOCUMENTO DE SEGURIDAD INTEGRADO

	Documento de Seguridad	
	Nombre del Sistema de Datos Personales	
	Fecha de elaboración	Fecha de la última Actualización
	Elaboró el documento	Aprobó
	(Nombre y firma)	(Nombre y firma)

DATOS GENERALES DEL SISTEMA

Nombre del sistema: [El nombre del sistema de datos personales, debe coincidir con el Acuerdo de Creación (en caso de que aplique) publicado en Gaceta Oficial de la Ciudad de México GOCDMX y/o con la inscripción en el Registro Electrónico de Sistemas de Datos Personales RESDP]

Fecha de publicación en la GOCDMX del Acuerdo de Creación: [Indicar la fecha de publicación en la Gaceta Oficial de la Ciudad de México del Acuerdo de creación del sistema de datos personales (en caso de que aplique)]

[Adjuntar como anexo copia de la publicación en la Gaceta Oficial de la Ciudad de México]

Fecha de inscripción en el RESDP: [Indicar la fecha de inscripción del sistema de datos personales en el RESDP]

Folio de inscripción en el RESDP: [Indicar el número de folio señalado en el Acuse de Registro del Sistema de Datos Personales]

[Adjuntar como anexo el Acuse de Registro del sistema de datos personales]

Fecha de publicación en GOCDMX del Acuerdo de Modificación: [Indicar la fecha de publicación del Acuerdo de modificación del sistema de datos personales, en la Gaceta Oficial de la Ciudad de México]

Fecha de última modificación en el RESDP: [Indicar la fecha de modificación del sistema de datos personales en el RESDP]

[Adjuntar como anexo los Acuses de edición del sistema de datos personales.

Normatividad aplicable para el tratamiento

(Señalar el nombre de la norma, los artículos; así como la fecha de publicación en GOCDMX o DOF).

I. INVENTARIO DE DATOS PERSONALES

Se debe crear y mantener actualizado un inventario de los datos personales o sus categorías. El inventario deberá identificar o estar vinculado con la información básica que permita conocer el tratamiento a que serán sometidos.

A.- Señalar el tipo de datos personales que contiene el Sistema (Datos Personales, Datos Personales Sensibles, o ambos).

B.- Además de listar cada uno de los datos personales recabados por ejemplo (nombres, apellido paterno, apellido materno, domicilio, estado civil), Datos laborales (correo electrónico institucional y teléfono institucional).

Aplicación

Las medidas de seguridad contenidas en el presente documento son de aplicación obligatoria para garantizar que los datos personales contenidos en el SDP denominado **(nombre del sistema)**, se ajuste a las disposiciones establecidas en la Ley.

Obtención

Las personas sobre las que se pretenden obtener datos de carácter personal son (_____)

La recolección de los datos personales que contiene es de carácter **(enlistar y agregar como anexo, los medios por los cuales se recaba la información, ya sean físicos, electrónicos o mixtos)**, con un nivel de seguridad **(señalar: básico, medio o alto)**, dado el tipo de datos personales que se contienen en el SDP referido.

Modo de tratamiento: El procesamiento de los datos personales se llevará a cabo a través de procedimientos **(físicos, electrónicos o mixtos)**

Medio de actualización: la actualización de los datos personales se llevará a cabo **(a petición del interesado, revisión periódica o mediante oficio)**

Finalidades del tratamiento

Finalidad y uso previsto: las finalidades de cada tratamiento de datos Personales **(Debe coincidir con la publicada en la GOCDMX, en caso de que aplique)**

- Uso:
- Acceso
- Manejo
- Aprovechamiento
- Monitoreo

Remisiones (Responsable – Encargados)

Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano

[Enlistar a la(s) persona(s) física(s) o jurídica(s), pública(s) o privada(s) ajena(s) al responsable y que tratan datos personales, a nombre y por cuenta del responsable. (Anexar copia del contrato, según sea el caso)]

Transferencias

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

[En su caso, enlistar los terceros receptores, a los que una normativa faculta la transferencia de datos personales, así como las finalidades que la justifican. Cuando las transferencias se realicen entre sujetos obligados se encuentre de manera expresa en una ley o tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos]

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. Interrelación (**Señalar si el SDP se interrelaciona con otro SDP del mismo Sujeto Obligado e indicar nombre del SDP y finalidad de la interrelación)**

El catálogo de los tipos de datos personales

Indicar el tipo de datos personales recabados en cada una de las categorías, indicando si son sensibles o no.

Ejemplo:

Datos identificativos: (Nombre, teléfono particular, edad, etc.)

Los datos personales del sistema (**en físico, automatizado o mixto)** se encuentran contenidos **(señalar donde se encuentran contenidos, series documentales. Anexar Catálogo de Disposición Documental)**

Ciclo de vida de los datos (Esta información deberá coincidir con lo que señala el Catálogo de Disposición Documental):

- En medio automatizado
- En archivo de trámite
- En archivo de concentración

Así como señalar si se contempla la transferencia de información al archivo histórico.

Nivel de seguridad: Indicar el nivel de seguridad aplicable de acuerdo al tipo de datos recabados:

- BÁSICO
- MEDIO
- ALTO

Medidas de seguridad: Describir las medidas de seguridad adoptada, aplicable a cada caso conforme a lo establecido en la Ley:

- Medidas de seguridad Administrativas
- Medidas de seguridad Físicas
- Medidas de seguridad Técnicas

Catálogo de las formas de almacenamiento:

Los expedientes del sistema de datos personales denominado **(nombre del sistema),** se encuentran resguardados en el inmueble localizado en **(domicilio de ubicación)**

Descripción general de la ubicación física y/o electrónica de los Datos personales. Se puede hacer uso de mapas, planos etc., para señalar la ubicación específica donde se resguarda el SDP.

(Insertar plano o mapa de ubicación del SDP y en su caso anexar el mapa de ubicación como un Anexo).

Lista de los servidores públicos que tienen acceso a los sistemas de tratamiento. (Responsable y usuarios involucrados en el tratamiento)

Solo los siguientes servidores públicos, podrán acceder a los contenidos del SDP, a objeto de dar paso al desarrollo de las funciones y atribuciones que les han sido conferidas.

NOMBRE:_____

CARGO:_____

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DE LOS SISTEMAS DE DATOS PERSONALES

Funciones y obligaciones del Encargado del Sistema:

La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Funciones: Además de lo que establece los artículos 55 y 56 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, indicar las funciones específicas que, de acuerdo a las atribuciones, le competen al Responsable de Seguridad del SDP.

Obligaciones: Además de lo que establece los artículos 55 y 56 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, indicar las obligaciones que de acuerdo a las atribuciones le competen al Responsable de Seguridad del SDP.

Funciones y obligaciones del (los) Usuarios (s) del Sistema

Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Funciones: Indicar, todas aquellas actividades que deberá llevar a cabo para el debido tratamiento y protección de los datos personales, con la finalidad de evitar que existan posibles vulneraciones.

Obligaciones: Indicar, las acciones que de conformidad con sus facultades deberá establecer para el debido resguardo y protección del o los SDP a su cargo: Lo anterior, de conformidad con lo establecido en la Ley de Datos.

Ejemplo:

FUNCIONES

1. Nombre de la Unidad Administrativa
2. Nombre del sistema

Responsable:

- Nombre:
- Cargo:
- Funciones, con relación al tratamiento de los datos personales en el manejo del sistema.
- Obligaciones: en cuanto al tratamiento de los datos personales en el sistema.

Encargado:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Usuario:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

OBLIGACIONES

3.- Nombre de la Unidad Administrativa
4.- Nombre del sistema

Responsable:

- Nombre:
- Cargo:
- Funciones con relación al tratamiento de los datos personales en el manejo del sistema.
- Obligaciones: en cuanto al tratamiento de los datos personales en el sistema.

Encargado:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Usuario:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

NOTA: Las funciones deben relacionarse con las de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de las facultades y atribuciones que le corresponden al Responsable del SDP de acuerdo con la Ley y los Lineamientos.

Si hay dos o más encargados del sistema y si existen dos o más usuarios del sistema, se recomienda agregar la información como Anexo al Documento de Seguridad, para hacer más fácil la integración del documento.

Establecer las obligaciones generales no incluidas en las categorías señaladas al principio de este apartado.

Ejemplo:

a) Guardar la debida secrecía sobre los datos personales que conozcan en el desarrollo de sus funciones, evitando su difusión y/o transmisión.

b) Informar al Responsable del Sistema o Responsable de Seguridad sobre cualquier incidencia que tenga conocimiento.

c) No dejar información visible cuando abandone su puesto, ya sea que se ausente de manera temporal o si hay alguna persona ajena a la Unidad Administrativa a la que esté adscrito.

d) Conservar el buen estado físico de los soportes documentales a que tengan acceso, con motivo del ejercicio de sus funciones.

e) Reportar alguna vulneración de los datos personales.

Establecer las políticas generales de seguridad que aplican a todo el personal o a persona ajena a la Unidad Administrativa que detenta el SDP

III. REGISTRO DE INCIDENCIAS

1.- Los datos de la incidencia:

a) Nombre de la persona que resolvió el incidente;

b) Método aplicado (elaboración y entrega de informe donde precise los soportes físicos y técnicos afectados y los recuperados).

c) Soportes físicos: (oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados)

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.

2.- Registro de la incidencia física o electrónica;

3.- Asegurar la incidencia;

4. Quién autorizó la recuperación de datos

REPORTE DE INCIDENCIAS

FORMATO (A)

Versión Anexo

Elaborado por:	Fecha elaboración	Aprobado por:	Fecha de aprobación:

En caso de presentarse una incidencia, deberá registrarse, tipo, fecha y hora, quien observó la incidencia, a quién se comunica y acciones a implementar para atender la incidencia.

Tipo de incidencia:
_____ El momento

en que se produjo: _____ Nombre y cargo de quién notifica la incidencia: _____ Nombre y cargo de quién recibe la notificación: _____ Las acciones que se implementan a consecuencia de la incidencia: _____ Soportes físicos: (oficios, expedientes, archiveros, ficheros, computadoras, discos duros robados o dañados) …… Soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados. _…….._____ _____ Quién autorizó la recuperación de datos: _____

En caso de que se presente la incidencia, se generará un acta circunstanciada de hechos.

FORMATO DE ACTA CIRCUNSTANCIADA DE HECHOS

Tipo de incidencia

FORMATO (B)

Una incidencia de seguridad puede ser cualquier incumplimiento de las disposiciones establecidas en el documento de Seguridad, y cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal en el sistema.

Estas, pueden ser generadas por el actuar de las personas que tienen acceso al sistema o a causa de desastres naturales y/o tecnológicos, así como a la comisión de delitos.

La Organización de las Naciones Unidas señala que los desastres se clasifican en:

1) Naturales; y
2) Tecnológicos.

IV. IDENTIFICACIÓN Y AUTENTIFICACIÓN

Mecanismos de identificación y autentificación

- El Responsable del sistema deberá elaborar una relación actualizada de los servidores públicos que tengan acceso autorizado al SDP. (Anexar relación) Indicar el Procedimiento de notificación o políticas de bajas de personal.
- El Responsable del sistema establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona que intente acceder al SDP. (Ejemplo: presentando identificación) [Incluir el procedimiento]

- Para SDP automatizados el Responsable del Sistema implementará procedimientos para el acceso seguro mediante asignación de claves y contraseñas al personal autorizado. Indicar el Procedimiento de creación y modificación de claves y contraseñas, señalando longitud, formato y contenido, así como inactivación de cuentas por baja de personal.

Medidas de seguridad implementadas para controlar el acceso de personas.

A las instalaciones:

a) identificarlo(a);
b) autenticarlo(a);
c) quien autoriza la identificación y la autenticación;
d) quien autoriza el acceso.

Al interior: medidas de seguridad implementadas para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema. (Oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)

a) identificarlo(a);
b) autenticarlo(a);
c) quien autoriza la identificación y la autenticación;
d) quien autoriza el acceso.

V. CONTROL DE ACCESO, GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPERACIÓN.

GESTIÓN DE SOPORTES

• Identificar el tipo de información que contienen los soportes físicos y electrónicos mediante el uso de etiquetas y ser inventariados. Sólo el personal autorizado podrá acceder a los soportes.

• Llevar un registro de la salida de las instalaciones u oficinas, de la información del SDP, la cual sólo podrá ser autorizada por la Responsable del mismo.

• Indicar el procedimiento para el traslado de información que contenga datos del sistema, debiendo adoptar medidas que eviten la sustracción, pérdida o acceso indebido a la misma. (Ejemplo: sobre cerrado con el sello o leyenda de CONFIDENCIAL y solo deberá de ser trasladado por personal autorizado)

• En caso de proceder alguna acción cuyo objeto sea la disposición documental autorizada, en cualquier medio, por destrucción o baja de la misma, cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando medidas eficaces que eviten completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento, con el fin de evitar el acceso a la información contenida

en el mismo, aplicando técnicas físicas o electrónicas.(Ejemplo: destruir en trituradora por el personal autorizado, los documentos físicos que contengan datos personales, formatear las computadoras que contengan información con datos personales, etc.)

• Se puede tomar la decisión de considerar medidas adicionales, si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente. Por ejemplo: el equipo 26 de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

• Señalar si el responsable del tratamiento de datos personales contrata o se adhiere a servicios, aplicaciones e infraestructura de cómputo en la nube, y otros servicios que impliquen el tratamiento de datos personales, el proveedor externo estará obligado a garantizar la protección de datos personales con los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

• En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos, de conformidad con la Ley de Datos.

• Descripción de perfiles del usuario y contraseñas implementados por el responsable para tener control de acceso mediante una red electrónica:

A.- El Control de acceso podrá ser

➢ Obligatorio;
➢ Discrecional;
➢ Rol desempeñado;
➢ Grupo perteneciente;
➢ De acuerdo al reglamento interior.

B.- Por el Perfil del usuario y contraseña para el manejo del sistema operativo podrá ser porque:

➢ Cuenta con un sistema operativo de red instalado en su equipo;
➢ Sistema operativo maneja rigurosos perfiles de usuario y contraseñas;
➢ El sistema operativo solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.

C.- Por el Perfil del usuario y contraseñas para el manejo del software podrá ser porque:

➢ El software maneja rigurosos perfiles de usuario y contraseñas;

➢ El software solo reconoce los nombres de usuarios y las contraseñas cuando los almacena.

D.- La administración de perfiles de usuario y contraseñas podrá ser por:

➢ Alta de nuevos perfiles;
➢ La creación de nuevos perfiles;
➢ Registro de la creación de nuevos perfiles.

E.- Acceso remoto al sistema de datos personales podrá ser porque:

➢ Requieren los usuarios acceso remoto al equipo de cómputo para trabajar con el sistema;
➢ Requiere el administrador acceso remoto al equipo para realizar tareas de mantenimiento.

RESPALDO Y RECUPERACIÓN

Establecer procedimientos conforme a las políticas existentes.

a) Copias de respaldo y recuperación.

• Procedimiento para realizar las copias de respaldo (establecer el procedimiento correspondiente).

- En soporte físico se procede a la digitalización de los documentos;
- En el soporte electrónico se realizará en discos, memorias externas, discos duros externos, etc.

- Periodo de realización; (lo establecerá el sujeto obligado)
- Verificación por parte del responsable. (al menos cada 6 meses)
- Establecer los procedimientos para recuperar datos contenidos en soportes electrónicos.

b) Pruebas con datos reales; (únicamente a sistemas informáticos y con previa copia de respaldo)

Se debe verificar la correcta aplicación y funcionamiento de los procedimientos para obtener copias de respaldo y de recuperación de los datos.

Las pruebas en nuevos sistemas informáticos diseñados para dar tratamiento al sistema, no se realizarán con datos reales, salvo que se asegure y garantice el nivel de seguridad correspondiente al tipo de datos tratados.

Previo a la realización de pruebas con datos reales, se debe elaborar una copia de respaldo.

VI. ANÁLISIS DE RIESGOS

Estudio de valor de los datos personales, el ciclo de vida, así como las causas, consecuencias, incidencias, amenazas y vulneraciones al sistema de tratamiento de datos personales.

- Benéfico; (nivel de riesgo inherente a los datos y numero de titulares que pueden ser afectados)
- Accesibilidad; (riesgo al número de accesos potenciales al sistema)
- Anónimo; (nivel de riesgo por el tipo de personas no identificables que tiene acceso al sistema)

• **Factores para Determinar las Medidas de Seguridad.** Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.

• **Valoración Respecto al Riesgo.** Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional, se compone de los siguientes pasos:

1. Identificar el tipo de nivel de seguridad y el valor de los datos personales, de acuerdo con su clasificación:

    ➢ El incumplimiento con las obligaciones legales y contractuales relacionadas con el titular;
    ➢ Vulneraciones de seguridad;
    ➢ Daño a la integridad de los titulares de datos personales;
    ➢ Daño a la reputación del Sujeto Obligado.
2. Identificar Amenazas: El valor y exposición;
3. Identificar Vulnerabilidades;
4. Identificar Escenarios de Vulneración y Consecuencias.

• **Criterios de aceptación del riesgo**. El Sujeto Obligado podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad sean consideradas como muy poco significativas.

Se debe expresar el beneficio o el riesgo estimado para la organización, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo, riesgos que pueden resultar del incumplimiento a la Ley que no pueden ser aceptados.

Se deben incluir múltiples umbrales, correspondientes a diferentes niveles de aceptación, previendo que los responsables acepten riesgos sobre esos niveles en circunstancias específicas.

El análisis de riesgos y las medidas de seguridad implementadas como resultado de lo arriba descrito, se deberá enfocar en la protección de datos personales contra daño,

pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones de conformidad con el artículo 3 fracción XVI de la Ley de Datos.

Ahora bien, la protección de datos personales deberá estar relacionada con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Para el tratamiento de los datos personales, se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo. Se pueden identificar tres tipos de tratamiento de datos: físicos, automatizados o mixtos.

De conformidad con el artículo 4 de la Ley de Datos, será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

[Nota: Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de riesgo, y el cual deberá de adaptarse a las condiciones de cada Sujeto Obligado. (Anexo 1)]

VII. ANÁLISIS DE BRECHA

Análisis de Brecha. Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener, que resultan necesarias para la protección de Datos Personales.

Los controles de seguridad, sin que sean limitativos, deben considerar los dominios siguientes:

- Políticas del Sistema de Gestión Sistema de Datos Personales;
- Cumplimiento legal;
- Estructura organizacional de la seguridad;
- Clasificación y acceso de los activos;
- Seguridad del personal;
- Seguridad física y ambiental (Aéreas seguras y protección de equipamiento);
- Gestión de comunicaciones y operaciones;
- Control de acceso;
- Desarrollo y mantenimiento de sistemas;
- Vulneraciones de seguridad;
- Seguridad institucional; (control de las transferencias de datos)
- Activos responsables; (asignación de responsable y clasificación)
- Seguridad de sistemas de información; (procesos de información, protección de archivos del sistema)
- Incidentes de seguridad en la información; (regularidad con la que se dan).

[Nota: Para mayor referencia, se anexa a la presente, el formato que servirá de guía de manera enunciativa más no limitativa, mismo que podrá utilizarse para llevar a cabo el análisis de brecha, y el cual deberá de adaptarse a las condiciones de cada

Sujeto Obligado. (Anexo 2)]

VIII. RESPONSABLE DE SEGURIDAD

Sera designado por el responsable y será el encargado de vigilar que se lleven a cabo todas las medidas de seguridad:

I. Desde el nivel básico;
II. Técnico;
III. Organizativo;
IV. Vigilar los centros de tratamiento de datos locales;
V. Equipos;
VI. Sistemas;
VII. Programas;
VIII. Personas que intervienen

IX. REGISTRO DE ACCESO Y TELECOMUNICACIONES

Registro de quien tiene acceso al sistema:

a) Nombre y cargo de quien accede al sistema;
b) Identificación del sistema;
c) Identificación del expediente;
d) Propósito del acceso;
e) Fecha de acceso;
f) Fecha de término de la consulta;
g) Hora de consulta.

Telecomunicaciones (transferencia telemática de datos) Se determina que datos pueden transferirse de manera que no puede ser manipulada.

I. Sistemas;
II. Bases de datos;
III. Imágenes;
IV. Archivos:

Control de acceso

- Listado de personal con acceso autorizado (Señalar por figura únicamente aquellos datos y recursos que precisen para el desarrollo de sus funciones)
- Bitácora de acceso, éstas se utilizan en los soportes físicos o electrónicos, debiendo establecer procedimiento para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el SDP, las cuales pueden contener la información siguiente:
  Nombre y cargo de quien accede
  Identificación del expediente

Propósito del acceso
Fecha de acceso
Hora de acceso
Fecha de devolución
Hora de devolución

Solamente el Responsable del Sistema podrá conceder, alterar o anular la autorización para el acceso al SDP.

X. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Para cumplimiento de lo establecido en el Artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los datos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en el nivel inaceptable de riesgo; y
VII. Los incidentes y vulneraciones de seguridad ocurridas.

Acciones que se toma para mantener actualizadas las medidas de seguridad y revisión de la mismas

a. Política se seguridad;
b. Cumplimiento de la normatividad;
c. Organización de la seguridad en la información;
d. Clasificación e identificación de inventarios;
e. Administración de incidentes;
f. Continuidad en las operaciones;
g. Gestión de comunicaciones y operaciones;
h. Adquisición, desarrollo, uso y mantenimiento del sistema de información;
i. Soportes físicos;
j. Soportes electrónicos;

XI. PLAN DE TRABAJO

El responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nueva o faltante.

Se elaborará respecto de los faltantes en el análisis de brecha

1. Fuga de información; (prevención)
2. Disociación; (cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor)
3. Bloquear y dar de baja puertos y servicios innecesarios en los equipos de cómputo;
4. Ampliación de medidas de seguridad en caso de detectar faltantes;
5. Equipos de cómputo obsoletos

XII. PLAN DE CAPACITACIÓN

Para los programas de capacitación, el responsable deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;
III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales; y
IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Calendario programático para llevar a cabo:

A. Capacitaciones integrales del personal que opera los sistemas;
B. Actualizaciones;
C. Fechas y duración de la capacitación;
D. Aéreas a capacitar;
E. Temas;
F. Mejoras implementadas;
G. Desaciertos y aciertos;
H. Oportunidades de mejora;
I. Retroalimentación

FORMATO (C)

Análisis de Riesgo Amenazas, vulnerabilidades y recursos involucrados				
Código	Pregunta o Control	¿Existe? SI	¿Existe? NO	Observaciones (acciones a realizar en caso de no contar con:
1.1	*¿Tienes identificado los datos personales?*			
1.2	*¿Tienes clasificados los datos personales?*			
1.3	*¿Tienes establecido el ciclo de vida de los datos personales?*			
1.4	*¿Tienes definido el tratamiento que se le da a cada uno de los datos personales?*			
1.5	*¿Tienes capacitaciones sobre qué hacer en caso de que los datos personales queden expuestos?*			
1.6	*¿Tienes un catálogo sobre las consecuencias negativas para los titulares de los datos personales?*			
1.7	*¿Tienes un plan reactivo en caso de sufrir la pérdida de datos personales?*			
1.8	*¿Tienes una bitácora de las causas que originaron el daño al sistema y por ende a los datos personales?*			
1.9	*¿Tienes registro de las amenazas surgidas durante la implementación, puesta en marcha y desarrollo del sistema, el cual contiene datos personales?*			
2. vulneraciones				
2.1	*¿Tienes una bitácora sobre vulneraciones sufridas en los datos personales?*			
2.2	*¿Tienes requerimientos regulatorios en caso de vulneración de los datos personales?*			
2.3	*¿Tienes una política a seguir en caso de daño al sistema por una vulneración de los datos personales?*			
2.4	*¿Tienes códigos de conducta del personal que trata datos personales?*			
2.5	*¿Tienes claro el beneficio para el*			

	atacante al obtener los datos personales?			
2.6	*¿Tienes un sistema de todas y cada una de las consecuencias que surgieron a raíz de la vulneración del sistema que contiene datos personales?*			
2.7	*¿Tienes procedimientos para actuar ante la vulneración de los sistemas de datos personales?*			
3. recursos involucrados				
3.1	*¿Tienes un software para descubrir la anonimidad del atacante de los datos personales?*			
3.2	*¿Tienes respaldos en el caso de que la información fue vulnerada?*			
3.3	*¿Tienes hardware y software para respaldar los datos personales?*			
3.4	*¿Tienes personal capacitado para llevar a cabo los respaldos hardware y software que contendrán los datos personales?*			
3.5	*¿Tienes calendario, con fechas para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			
3.6	*¿Tienes asesoría externa para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware y software en los que se almacenan datos personales?*			

FORMATO (D)

Análisis de Brecha Medidas de seguridad existentes y medidas de seguridad faltantes				
Código	Pregunta o Control	¿Existe? SI	¿Existe? NO	Observaciones
1.- Medidas de seguridad basadas en la cultura del personal				
1.1	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
1.1.1	*Política de escritorio limpio*			
1.1.2	*Hábitos de cierre y resguardo*			
1.1.3	*Impresoras, escáneres, copiadoras y*			

	buzones limpios			
1.1.4	*Gestión de bitácoras, usuarios y acceso*			
2	*¿Tienes mecanismos para eliminar de manera segura la información?*			
2.1	*Destrucción segura de documentos*			
2.2	*Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico*			
2.3	*Fijar periodos de retención y destrucción de información*			
2.4	*Tomar precauciones con los procedimientos de re-utilización*			
2.5	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			
3.- Medidas de seguridad basadas en la cultura del personal				
3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			
3.2	Fomentar la cultura de la seguridad de la información			
3.3	Difundir noticias en temas de seguridad			
3.4	Prevenir al personal sobre la *Ingeniería Social*			
3.5	Asegurar la protección de datos personales en subcontrataciones			
4	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*			
4.1	Tener un procedimiento de notificación.			
4.2	Realizar revisiones y auditorías.			
5	*¿Realizas respaldos periódicos de los datos personales?*			
6.- Medidas de seguridad en el entorno de trabajo físico				
6.1	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*			
6.1.1	Alerta del entorno de trabajo.			
6.1.2	Mantener registros del personal con acceso al entorno de trabajo			
6.2.1	*¿Tienes medidas de seguridad para evitar el robo?*			
6.2.2	Cerraduras y candados			

6.2.3	Elementos disuasorios.			
6.2.4	Minimizar el riesgo oportunista.			
6.3	*¿Cuidas el movimiento de información en entornos de trabajo físicos?*			
6.3.1	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico			
6.3.2	Mantener en movimiento sólo copias de la información, no el elemento original			
6.3.3	Usar mensajería certificada			
7.- Medidas de seguridad en el entorno de trabajo digital				
7.1	*¿Realizas actualizaciones al equipo de cómputo?*			
7.2	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*			
7.3	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*			
7.3.1	Uso de contraseñas y/o cifrado			
7.3.2	Uso de contraseñas solidas			
7.3.3	Bloqueo y cierre de sesiones			
7.3.4	Administrar usuarios y accesos			
7.4	*¿Revisas la configuración de seguridad del equipo de cómputo?*			
7.5	*¿Tienes medidas de seguridad para navegar en entornos digitales?*			
7.5.1	Instalar herramientas antimalware y de filtrado de tráfico			
7.5.2	Reglas de navegación segura			
7.5.3	Reglas para la divulgación de información			
7.5.4	Uso de conexiones seguras			
7.6	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*			
7.6.1	Validación del destinatario de una comunicación			
7.6.2	Seguridad de la información enviada y recibida			