Instituto de Acceso
a la Información Pública
y Protección de Datos Personales
del Estado de Oaxaca

Departamento Protección de Datos Personales y Archivos

¿Qué es y cómo elaborar un Documento de Seguridad?:

GUÍA PARA SUJETOS OBLIGADOS

Contenido

¿Qué es Documento de Seguridad? 3

¿Cuáles son las finalidades del Documento de Seguridad? 3

¿Para qué sirve un Documento de Seguridad? 3

¿Qué hacer para implementar de forma adecuada un Documento de Seguridad al interior de nuestro Sujeto obligado? 4

¿Cuáles son los pasos para la elaboración de un Documento de Seguridad? 5

¿Cuáles son los elementos indispensables del Documento de Seguridad? 6

¿Qué es un Inventario de Datos Personales y de sistemas de tratamiento? 7

¿Cómo establezco las funciones y obligaciones de las personas que traten datos personales? 12

¿Cómo se elabora la Bitácora de Responsables, Encargados y Usuarios de los Sistemas de Datos Personales? 12

Apartados destinados al establecimiento de roles y responsabilidades del personal en materia de protección de datos personales 13

I. Transmisiones de datos personales 13

II. Resguardo de sistemas de datos personales con soportes físicos * 16

IV. Registro de incidentes 17

V. Acceso a las instalaciones 17

VI. Actualización del sistema de datos personales 18

VII. Perfiles de usuario y contraseñas 19

VIII. Procedimientos de respaldo y recuperación de datos 20

¿Qué es y cómo se elabora un análisis de riesgo? 21

¿Qué es y cómo se elabora un análisis de brecha? 22

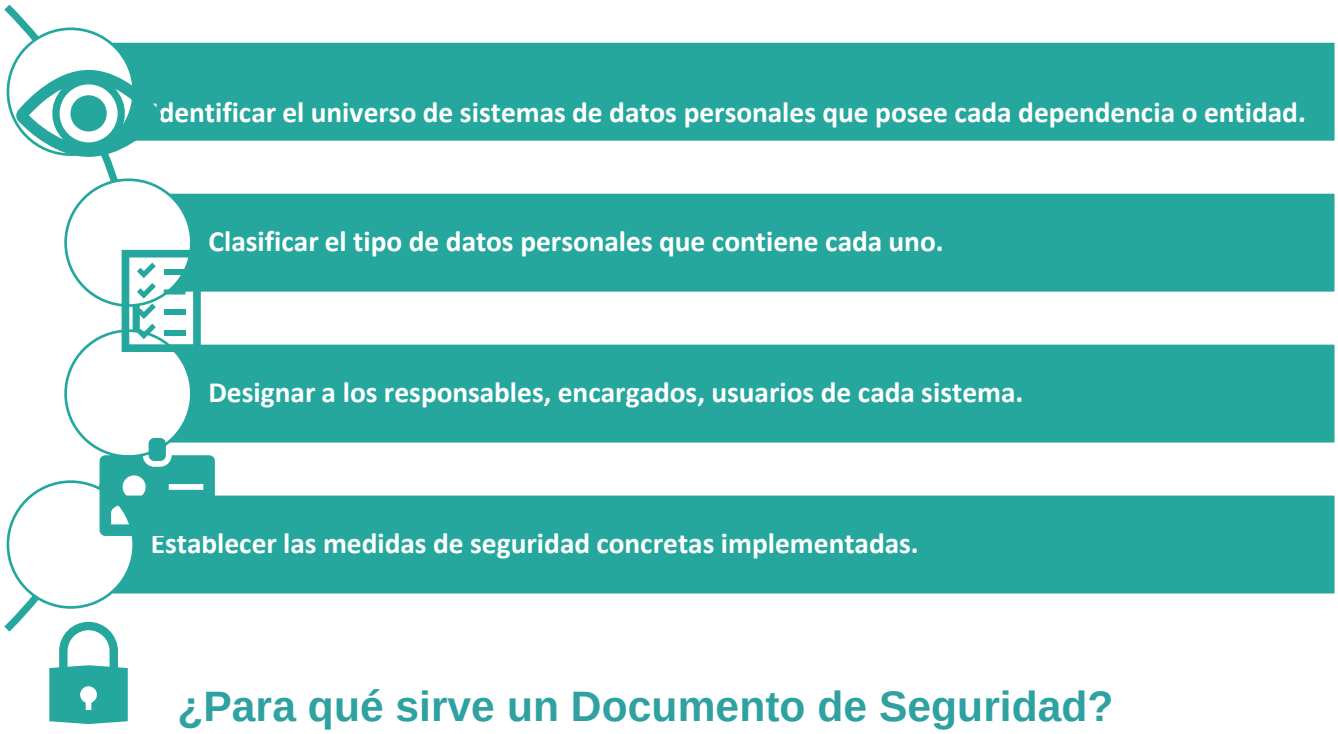
¿Cuáles son las partes finales del documento? 24

Glosario de términos y Acrónimos 27

¿Qué es Documento de Seguridad?

Documento elaborado por el sujeto obligado que contiene las medidas de seguridad administrativa, física y técnica aplicables a sus sistemas de datos personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen. (Art. 3 LPDPPSO).

¿Cuáles son las finalidades del Documento de Seguridad?



¿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.

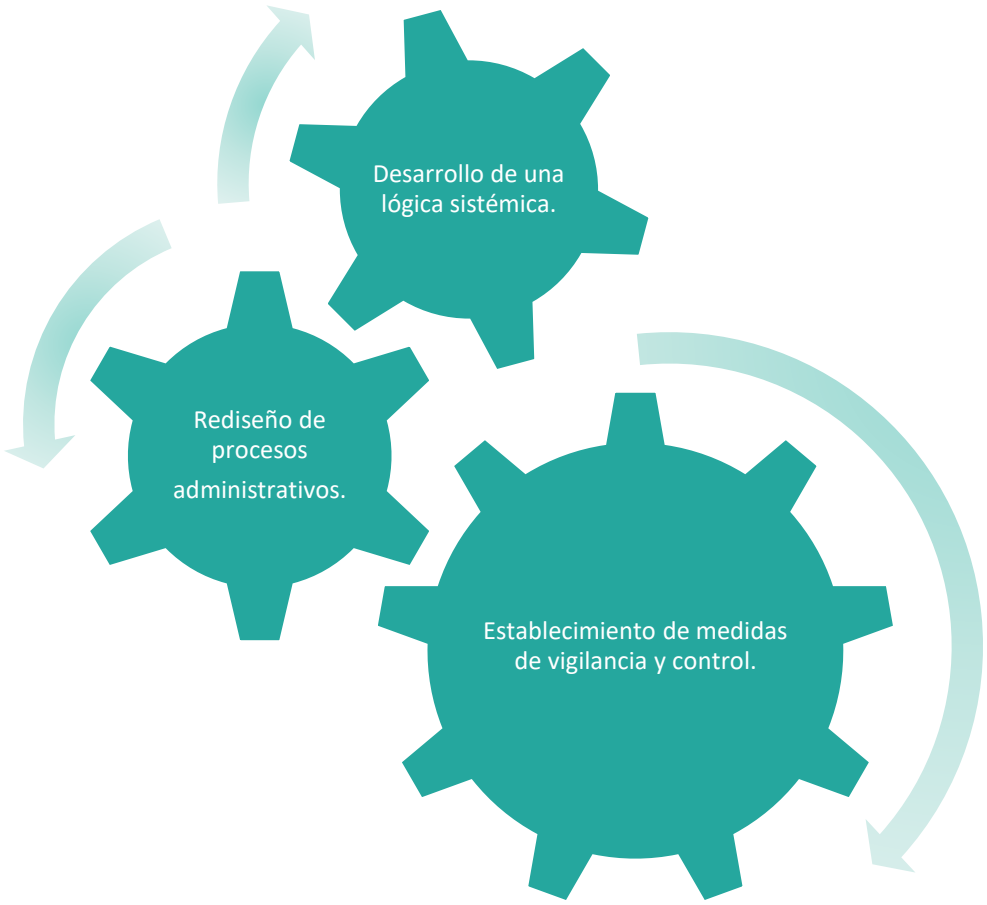
Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

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.**

¿Qué hacer para implementar de forma adecuada un Documento de Seguridad al interior de nuestro Sujeto obligado?

.



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

De un tratamiento a un sistema de datos personales.

Los sistemas de datos se agrupan a un Sistema Institucional.

Establecimiento de una Política Institucional de Protección de Datos Personales.

Identificar el universo de sistemas de datos personales que poseen.

Identificar entre datos personales y datos personales sensibles.

Designar responsables y encargados de cada sistema.

Establecer las medidas de seguridad necesarias para proteger los sistemas.

¿Cuáles son los elementos indispensables del Documento de Seguridad?

- El inventario de datos personales y de los sistemas de tratamiento.
- Las funciones y obligaciones de las personas que traten datos personales.
- Los Análisis de Riesgo y brecha.
- El plan de trabajo.
- Los mecanismos de monitoreo y revisión de las medidas de seguridad.
- El programa general de capacitación.

¿Qué es un Inventario de Datos Personales y de sistemas de tratamiento?

Inventario de datos personales: se refiere a qué **datos personales** se tienen, cuál tipo son (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.

FORMATO GUÍA: INVENTARIO DE DATOS PERSONALES.

Marcar con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos administrativos de su Unidad Administrativa.

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos de identificación y contacto.			
Nombre:			
Estado Civil:			
Registro Federal de Contribuyentes (RFC):			
Clave Única de Registro de Población (CURP):			
Lugar de nacimiento:			
Fecha de nacimiento:			
Nacionalidad:			
Domicilio:			
Teléfono particular:			
Teléfono celular:			
Correo electrónico:			
Firma autógrafa:			
Firma electrónica:			
Edad:			

Fotografía:			
Referencias personales:			
Datos sobre características físicas.			
Color de piel:			
Color de cabello:			
Señas particulares:			
Estatura:			
Peso:			
Cicatrices:			
Tipo de sangre:			
Datos biométricos.			
Imagen del iris:			
Huella dactilar:			
Palma de la mano:			
Datos laborales.			
Puesto o cargo que desempeña:			
Domicilio de trabajo:			
Correo electrónico institucional:			
Teléfono institucional:			
Referencias laborales:			
Información generada durante los procedimientos de reclutamiento, selección y contratación:			
Experiencia/Capacitación laboral:			
Datos académicos.			
Trayectoria educativa:			

Títulos:			
Cédula profesional:			
Certificados:			
Reconocimientos:			
Datos migratorios.			
Entrada al país:			
Salida del país:			
Tiempo de permanencia en el país:			
Calidad migratoria:			
Derechos de residencia:			
Aseguramiento:			
Repatriación.			
Datos patrimoniales y/o financieros.			
Bienes muebles:			
Bienes inmuebles:			
Información fiscal:			
Historial crediticio/Buró de crédito:			
Ingresos:			
Egresos:			
Cuentas bancarias:			
Números de tarjetas de crédito:			
Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin):			
Seguros:			
Afores:			

Datos sobre pasatiempos, entretenimiento y diversión.			
Pasatiempos:			
Aficiones:			
Deportes que practica:			
Juegos de su interés:			
Datos legales.			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros):			
Otros datos personales (mencionar).			
Datos personales recabados:	**Existente.**	**Necesario.**	**No necesario.**

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos personales sensibles.			
Datos sobre la ideología.			
Posturas religiosas/ ideológicas/morales/ filosóficas:			
Pertenencia a un partido/Posturas políticas:			
Pertenencia a un sindicato:			
Datos de salud.			
Estado de salud físico presente, pasado o futuro:			

Estado de salud mental presente, pasado o futuro:			
Información genética:			
Datos sobre vida sexual.			
Preferencias sexuales:			
Prácticas o hábitos sexuales:			
Datos de origen étnico o racial.			
Pertenencia a un pueblo, etnia o región:			
Otros datos personales (mencionar).			

Descripción de los tipos de soporte de los Sistemas de Datos Personales

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
Tipo de Soporte: **Físico o electrónico:**	
Descripción del soporte:	
Características del lugar donde se resguardan los soportes: [Describir el lugar en el que físicamente se encuentran los soportes del sistema]:	

¿Cómo establezco las funciones y obligaciones de las personas que traten datos personales?

Obligaciones comunes de todos los responsables de proteger datos personales.

- Conocer la privacidad de todos los **datos** que manejan y, por lo tanto, su obligación de mantener el secreto de dicha información.
- Hacer uso de los datos únicamente para los fines para los cuales han sido recabados.

Los roles y funciones del personal con respecto al tratamiento y protección de los datos personales deben estar descritos en una bitácora donde se establezcan los responsables, encargados y usuarios de los datos personales.

¿Cómo se elabora la Bitácora de Responsables, Encargados y Usuarios de los Sistemas de Datos Personales?

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
Responsable:	
Nombre:	
Cargo:	
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	
Encargados:	
Nombre:	

Cargo:	
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	
Usuarios:	
Nombre:	
Cargo:	
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema].	

Apartados destinados al establecimiento de roles y responsabilidades del personal en materia de protección de datos personales

I. Transmisiones de datos personales

PARA SOPORTES FÍSICOS.

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
I. Trasmisiones de Datos Personales.	
1.1. Trasmisiones de Datos Personales en soportes físicos.	
Descripción del soporte:	Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria.
Características del paquete:	Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega.

Mecanismos para la entrega:	Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial.
Mecanismos para la notificación de vulneraciones:	Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura.
Acuse de recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona.

PARA TRASLADO FÍSICO DE SOPORTES ELECTRÓNICOS

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
I. Trasmisiones de Datos Personales.	
1.2. Trasmisiones de Datos Personales en soportes electrónicos, trasladados de forma física.	
Descripción del soporte:	Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria.
Características del paquete:	Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega.
Mecanismos para la entrega:	Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial.
Mecanismos para la notificación de vulneraciones:	Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura.
Acuse de recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona.
Tipo de cifrado:	Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el

	tipo de algoritmo utilizado y la longitud de la llave (o clave).

PARA SOPORTES ELECTRÓNICOS

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
I. Trasmisiones de Datos Personales.	
1.3. Trasmisiones de Datos Personales en soportes electrónicos.	
Procedimiento de Trasmisión:	
Tipo de cifrado:	Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave).
Canal de Trasmisión:	Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transmisiones protegidas utilizado.
Mecanismos para detectar intrusiones:	Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones.
Acuse de Recibido:	Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales.
Comunicación con el sistema de protección de datos del remitente:	Deberá señalar si el remitente registra la o las transmisiones en su bitácora, así como en el Sistema Persona

II. Resguardo de sistemas de datos personales con soportes físicos *

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
II. Tipo de Soporte del sistema:	Físico.
Medidas de seguridad implementadas:	Señalar las medidas de seguridad que ha implementado el sujeto obligado para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
Personal autorizado para el acceso al sistema:	Señalar en un listado las personas que tienen acceso a los soportes físicos del sistema.

III. Bitácoras para accesos y operación cotidiana

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
III. Bitácoras para accesos y operación cotidiana.	
Los datos que se registran en las bitácoras:	
Datos de acceso:	Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida.
Soporte físico:	Número o clave del expediente utilizado.
Soporte Electrónico:	Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

IV. Registro de incidentes

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
IV. Registro de Incidentes.	
Persona que resolvió el incidente:	
Metodología aplicada:	Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida.
Soporte físico:	Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados.
Soporte Electrónico:	Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.
Autorización a la recuperación de datos:	Nombre del responsable quien autoriza la recuperación de los datos.

V. Acceso a las instalaciones

PARA DESCRIBIR LA SEGURIDAD PERIMETRAL

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
V. Acceso a las instalaciones.	
Descripción de las medidas generales de seguridad perimetral:	
Proceso de identificación para el ingreso:	
Proceso de autentificación para el ingreso:	
Proceso de autorización para el ingreso:	

PARA DESCRIBIR LA SEGURIDAD AL INTERIOR

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
V. Acceso a las instalaciones.	
Descripción de las medidas generales de seguridad al interior:	
Proceso de identificación para el ingreso:	
Proceso de autentificación para el ingreso:	
Proceso de autorización para el ingreso:	

VI. Actualización del sistema de datos personales

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
VI. Mecanismo de actualización del sistema.	
Descripción del mecanismo:	Establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenido en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

VII. Perfiles de usuario y contraseñas

A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
VII. Perfiles de usuario y contraseñas.	
Modelo de control de acceso:	¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? ¿Es discrecional (matriz de control de acceso)? ¿Está basado en roles (perfiles) o grupos? ¿Está basado en reglas?
Perfiles de usuario y contraseñas en el sistema operativo de red:	¿Cuenta con un sistema operativo de red instalado en sus equipos? ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuándo los almacena?
Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:	¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Administración de perfiles de usuario y contraseñas:	¿Quién da de alta nuevos perfiles? ¿Quién autoriza la creación de nuevos perfiles? ¿Se lleva registro de la creación de nuevos perfiles?
Acceso remoto al sistema de datos personales:	¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? ¿Cómo se evita el acceso remoto no autorizado?

VIII. Procedimientos de respaldo y recuperación de datos

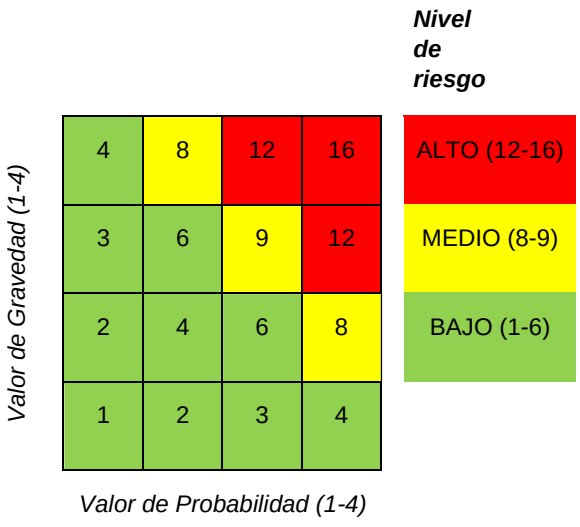
A. [Denominación de la Unidad administrativa A]:	
A1. [Nombre del sistema A1]:	
VIII. Procedimiento de respaldo y recuperación de los datos.	
Tipo de respaldo:	Señalar si realiza respaldos completos, diferenciales o incrementales.
Tipo de medios:	El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad.
Especificaciones sobre el almacenamiento:	Cómo y dónde archiva esos medios.
Nombre del responsable de las operaciones de respaldo:	

Una vez que hemos establecido esto, debemos analizar el estado actual y futuro de nuestros sistemas de datos personales. Esto significa realizar un análisis de riesgo y un análisis de brecha.

¿Qué es y cómo se elabora un análisis de riesgo?

Análisis previo que se debe de dar a todo nuevo tratamiento de **datos personales** con la principal finalidad de establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de las personas afectadas.

MATRIZ DE ANÁLISIS DE RIESGOS.						
A. [Denominación de la Unidad administrativa A].						
IDENTIFICACIÓN		**ANÁLISIS**		**EVALUACIÓN**		**TRATAMIENTO O CONTROL OPERACIONAL**
A1. [Nombre del sistema A1]	**RIESGO**	**PROBABILIDAD**	**GRAVEDAD**	**CALIFICACIÓN**	**NIVEL DEL RIESGO**	
Nombre de la base de datos personales mencione el nombre con el cual identificará esa base.	Describa claramente el o los posibles riesgos.	Establezca el valor de 1 a 4 según la probabilidad de ocurrencia del riesgo o riesgos anteriormente explicados. 1 siendo nada probable y 4 muy probable.	Establezca el valor de 1 a 4 según la gravedad del riesgo o riesgos mencionados anteriormente. 1 siendo nada grave y 4 muy grave.	Multiplique el valor de probabilidad por el valor de la gravedad.	Establezca el mismo de acuerdo a la calificación obtenida (alto, medio o bajo), esto de acuerdo a la tabla de colores verde, amarillo y rojo.	Describa el tratamiento o el control que se aplicará al o los riesgos, para que este se prevenga, reduzca o elimine.



¿Qué es y cómo se elabora un análisis de brecha?

Análisis de las medidas de seguridad existentes y aquellas faltantes, que resultan necesarias para la protección de los datos personales.

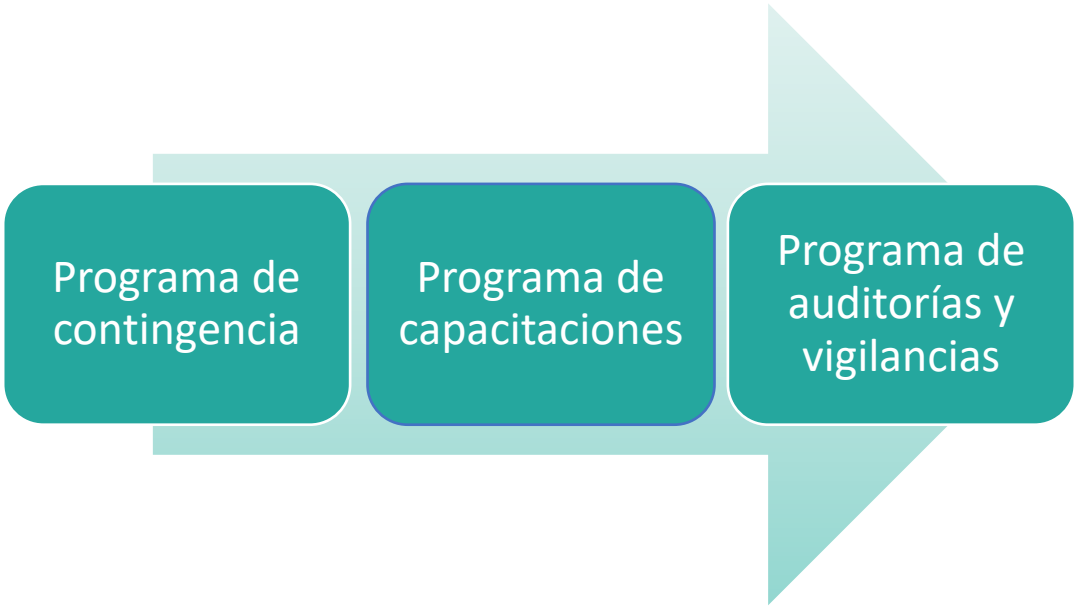
Análisis de Brecha.			
A. [Denominación de la Unidad administrativa A].			
A1. [Nombre del sistema A1].			
(Medidas de seguridad existentes VS medidas de seguridad faltantes).			
Pregunta o Control.	**¿Existente?**		
	SI	**NO**	**Observaciones.**
Medidas de seguridad basadas en la cultura del personal.			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?			
Política de escritorio limpio.			
Hábitos de cierre y resguardo.			
Impresoras, escáneres, copiadoras y buzones limpios.			
¿Tienes mecanismos para eliminar de manera segura la información?			
Destrucción segura de documentos.			
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico.			
Fijar periodos de retención y destrucción de información.			
Tomar precauciones con los procedimientos de reutilización.			
Informar al personal sobre sus deberes mínimos de seguridad y protección de datos.			
Fomentar la cultura de la seguridad de la información.			
Asegurar la protección de datos personales en subcontrataciones.			

¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?			
Tener un procedimiento de notificación.			
¿Realizas respaldos periódicos de los datos personales?			
Medidas de seguridad en el entorno de trabajo físico.			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			
Mantener registros del personal con acceso al entorno de trabajo.			
¿Tienes medidas de seguridad para evitar el robo?			
Cerraduras y candados.			
Elementos disuasorios.			
¿Cuidas el movimiento de información en entornos de trabajo físicos?			
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico.			
Mantener en movimiento sólo copias de la información, no el elemento original.			
Usar mensajería certificada.			
Medidas de seguridad en el entorno de trabajo digital.			
¿Realizas actualizaciones al equipo de cómputo?			
¿Revisas periódicamente el software instalado en el equipo de cómputo?			
¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?			
Uso de contraseñas y/o cifrado.			
Bloqueo y cierre de sesiones.			
Administrar usuarios y accesos.			
¿Revisas la configuración de seguridad del equipo de cómputo?			
¿Tienes medidas de seguridad para navegar en entornos digitales?			

Reglas de navegación segura.			
Uso de conexiones seguras.			
¿Cuidas el movimiento de información en entornos de trabajo digitales?			
Seguridad de la información enviada y recibida.			

Finalmente, se debe establecer un plan de trabajo que incluya: un programa de contingencias, un programa de capacitaciones y un programa de vigilancia y auditorías.

¿Cuáles son las partes finales del documento?



Programa de contingencia.

Programa de contingencia	
Programa de contingencia:	Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
Mecanismos para probar su eficacia:	Modelos, simulacros, ataques controlados, simulaciones.
Sitios alternos de resguardo:	El tipo de sitio (caliente, tibio o frío); Si el sitio es propio o subcontratado con un tercero.
Procedimiento detallado ante vulneraciones y contingencias:	
Tiempo de reacción:	

Programa de capacitación.

A. [Denom **Programa de Capacitación** Unidad administrativa A]	
Programa de capacitación:	
Periodicidad:	Anual, Semestral, Trimestral, etc.
Unidades administrativas a las que va dirigido:	
Temas para abordar y cronograma:	
Responsable del programa:	
Medios de verificación del aprendizaje:	

Programa de auditorías y vigilancias.

A. [Denom **Programa de Auditoria y vigilancia** inación de la Unidad administrativa A]	
Programa de Auditoría y vigilancia:	
Periodicidad:	Anual, Semestral, Trimestral, etc.
Unidades administrativas a las que va dirigido:	
Responsable de la ejecución:	
Manejo de la información reportada:	

PARTES FINALES DEL DOCUMENTO DE SEGURIDAD.

1. **Mecanismos para la supresión de un Sistema de Datos Personales.**
2. **Aprobación del documento por el Comité de Transparencia.**
3. **Anexos técnicos.**

NOTA: la divulgación o publicación total del documento de seguridad constituye en sí, una vulneración de los sistemas de datos personales contenidos en el mismo, por lo que deben elaborarse versiones públicas que disminuyan el riesgo de vulneraciones a los datos personales.

Glosario de términos y Acrónimos

- **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos.

- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

- **IAIP:** Instituto de Acceso a la Información y Protección de Datos Personales del Estado de Oaxaca.

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

- **LPDPPSO:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.

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

- **Responsable:** Cualquier autoridad, dependencia, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del Estado, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales, es decir, aquellos que tengan carácter de sujeto obligado en términos del artículo 3 de la LPDPPSO.

- **Titular:** La persona física a quien corresponden los datos personales.

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

- **Tratamiento:** 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.