OGAIPO

Órgano Garante de Acceso a la Información Pública, Transparencia, Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca

GUÍA PARA SUJETOS OBLIGADOS

ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

CONTENIDO

1. ¿QUÉ ES EL 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. (Artículo 3 Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Oaxaca)

2. ¿PARA QUÉ SIRVE UN DOCUMENTO DE SEGURIDAD?

Contribuye a establecer y mantener medidas de seguridad eficaces de carácter administrativo, físico y técnico para la protección de datos personales en su posesión, con el objeto de impedir que cualquier tratamiento de datos personales sea contrario a lo establecido en la normatividad aplicable.

3. ELEMENTOS DEL DOCUMENTO DE SEGURIDAD

1. Inventario de datos personales y sistemas de tratamiento
2. Funciones y obligaciones de las personas que tratan datos personales
3. Análisis de riesgos
4. Análisis de brecha
5. Plan de trabajo
6. Mecanismos de monitoreo y revisión de medidas de seguridad
7. Programa General de Capacitación

4. PROCESO PARA ELABORAR UN DOCUMENTO DE SEGURIDAD

Fase 1	**Planeación y diagnóstico**	• Definir alcance y objetivos. • Elaboración de diagnóstico del tratamiento de datos personales. • Reunión con titulares de las áreas administrativas del responsable.

La o el Oficial de Protección de Datos Personales del Sujeto obligado o persona del servicio público que funja como tal; será quien defina el alcance y objetivos del Documento de Seguridad apegado a los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.

Deberá solicitar a las áreas que forman parte del responsable lo siguiente:

- Si recaban datos personales.
- Cuál es la finalidad por la cual recaban datos personales.
- Normatividad que aplica al sujeto obligado.

Fase 2	**Desarrollo**	• Elaboración del inventario de datos personales con los resultados del diagnóstico. • Identificación de funciones y obligaciones de las personas del servicio público que realizan tratamiento de datos personales. • Realización del análisis de riesgos e identificación de medidas de seguridad. • Realización del análisis de brecha para la identificación de condiciones adecuadas a implementar. • Creación de políticas internas y medidas preventivas, para la gestión, tratamiento y protección de los datos personales.

Contando con la información previamente solicitada deberán llevar a cabo lo siguiente:

1) Inventario de datos personales y sistemas de tratamiento

Para elaborar el inventario de datos personales de cada tratamiento se deberán considerar, los siguientes elementos:

1.1. Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.

Área	Medio de Recolección
Ejemplo: Recursos humanos	Ejemplo: Físico

Medios físicos: soporte papel: listas de asistencia, formularios de registro.
Medios electrónicos: bases de datos, páginas web, sitios web.

1.2. Las finalidades de cada tratamiento de datos personales.

Área	Finalidades del tratamiento
Ejemplo: Recursos humanos	Ejemplo: Integrar expedientes del personal

Finalidades: Actividades y/o procedimientos que realizan y para los cuales requieren recabar datos personales, siendo estas lícitas, legítimas y concretas.

1.3. Catálogo de los tipos de datos personales que se tratan y si son

Área	Tipos de datos personales	Sensibles
Ejemplo: Recursos humanos	Identificación Patrimoniales Académicos Bancarios Familiares	X
Ejemplo: Recursos financieros	Identificación	

Categorías de datos personales: Identificación, patrimoniales, académicos, bancarios, familiares, biométricos, características físicas.

1.4. Existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados.

Área	Medidas de seguridad existentes
Ejemplo: Recursos humanos	Indicar cada una de las medidas de seguridad con las que se cuenta al interior del responsable. Administrativa: Físicas Técnicas:
Ejemplo: Recursos financieros	Administrativa: Física: Técnica:

Posterior a la identificación de las medidas de seguridad existentes, el usuario de datos personales deberá determinar si es necesario implementar nuevas medidas de seguridad.

Unidad Administrativa	Medidas de seguridad a implementar	Tipo de medida (administrativa, física o técnica)
Dirección administrativa	Colocar chapa con llave en el área de recursos humanos	Física

1.5. Ciclo de vida de los datos personales.

Para determinar el ciclo de vida de los datos personales se debe considerar lo siguiente:

- La obtención de los datos personales
- El almacenamiento de los datos personales
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.

- La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.
- El bloqueo de los datos personales, en su caso.
- La cancelación, supresión o destrucción de los datos personales.

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente

Tomando en cuenta lo anterior y para garantizar la adecuada conservación de los documentos que contienen datos personales, la o el usuario de los datos personales deberá identificar las series que contengan datos personales tomando en cuenta el Cuadro de Clasificación Archivística y el Catálogo de disposición documental; esto permitirá establecer los plazos de conservación de los datos personales que se recaban y se tratan.

Unidad Administrativa	Finalidades	Series documentales	Valores documentales	Plazos de Conservación*	
				Trámite	Concentración
Ejemplo: Dirección Administrativa	Nóminas	9C.4	Administrativo – contable y legal	2 años	3 años

2) Funciones y obligaciones de las y los usuarios que tratan datos personales

Establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de las y los servidores públicos que traten datos personales al interior del sujeto obligado.

Unidad Administrativa	Administrador	Usuario	Funciones
Dirección de Administración	Nombre del titular de la dirección	María Juárez	Realizar los procesos administrativos en materia de recursos humanos

Realización del análisis de riesgos e identificación de medidas de seguridad

3) Análisis de riesgo

Para dar cumplimiento al artículo 33, fracción IV de la Ley General de protección de datos personales, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de datos personales.
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- Los factores previstos en el artículo 32 de la Ley General (medidas de seguridad).

Para determinar las medidas de seguridad a implementar se analizarán los siguientes puntos:

a. **Beneficio para el atacante:** Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados. (beneficio económico por venderlos o usarlos).

b. **Accesibilidad para el atacante:** Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados. (miles de personas pueden acceder a la vez a una base de datos a través de un sitio web).

c. **Anonimidad del atacante:** Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados. (internet es un medio más anónimo que presentarse físicamente a las instalaciones de la institución).

Unidad Administrativa	Número de titulares de datos personales
Indicar el área que recaba datos personales	Indicar el número de titulares (personas) de las cuales recaban datos personales
Total de titulares de datos personales	**Sumar el número de titulares (personas) de las cuales recaban datos personales**

Lo anterior permitirá determinar el nivel de riesgo al que están expuestos los datos personales que recaban, de acuerdo a lo siguiente:

Tabla guía

Tipo de dato	Nivel de Riesgo Inherente
Identificación	Bajo
Académicos	Bajo
Patrimoniales	Inherente medio
Familiares	Inherente medio
Bancarios	Inherente reforzado
Biométricos	Inherente alto

4) Análisis de brecha

Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el Responsable deberá considerar lo siguiente:

- Las medidas de seguridad existentes y efectivas.
- Las medidas de seguridad faltantes.

4.1. Medidas de seguridad existentes

Área	Medidas de seguridad existentes
Dirección administrativa	Físicas: Técnicas: Administrativas:
Dirección Jurídica	Físicas: Técnicas: Administrativas:

4.2. Medidas de Seguridad faltantes

Adicional a las medidas de seguridad propuestas por cada área se sugiere fortalecer o implementar las siguientes medidas de seguridad

Medidas de seguridad a implementar	Tipo de medida de seguridad
	Administrativa Física Técnica

Fase 3	**Implementación**	• Elaboración del Plan de Trabajo para instrumentar las medidas necesarias en el Documento de Seguridad. • Implementar el plan de trabajo diseñado.

5) Plan de Trabajo

Posterior a la revisión de las acciones a implementar y de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, deberán priorizar las medidas de seguridad más relevantes e inmediatas que es necesario establecer de manera mensual, bimestral o trimestral e incluir en su Plan de Trabajo las acciones a realizar.

	Indicar si la acción se realizara de manera mensual, bimestral o trimestral		
Acciones a implementar	**Mensual**	**Bimestral**	**Trimestral**
Realizar actividades de capacitación dirigida a las personas del servicio público del sujeto obligado de acuerdo al tratamiento que realicen de datos personales.		X	

Fase 4	**Control**	• Establecimiento de procesos de evaluación continúa y monitoreo de las medidas implementadas y/o riesgos que se pudieran generar. (Verificación, auditoria). • Diseño de programas de capacitación para el personal que interviene en el tratamiento de los datos personales.

6) Monitoreo y supervisión periódica de las medidas de seguridad implementadas

El responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos, medidas de seguridad establecidos, y en su caso, implementar mejora de manera continua.

Para poder monitorear lo anterior, deben tomar en cuenta lo siguiente:

a. Los nuevos activos que se incluyan en la gestión de riesgos

b. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica.

c. Las nuevas amenazas qué podrían estar activas dentro y fuera de la organización y que no han sido valoradas.

d. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

e. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

f. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

g. Los incidentes y vulneraciones de seguridad ocurridas.

Tomando en cuenta lo anterior, deberá indicar el tiempo en el que realizará el monitoreo y/o revisión de las medidas de seguridad implementadas.

	Indicar si la acción se realizara de manera mensual, bimestral o trimestral		
Monitoreo de las medidas de seguridad	**Mensual**	**Bimestral**	**Trimestral**
			X

7) Programa general de capacitación

El responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a las y los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

	Indicar si la acción se realizara de manera mensual, bimestral o trimestral		
Temas de capacitación	**Mensual**	**Bimestral**	**Trimestral**
	X		

5. ¿CÓMO INTEGRAR EL DOCUMENTO DE SEGURIDAD?

1. La o el Oficial de Protección de Datos Personales y/o el Responsable de la Unidad de Transparencia, deberá trabajar de manera conjunta con las áreas y solicitarles la información tomando en cuenta cada una de las fases establecidas en esta guía.

2. Posterior a que las áreas cuenten con la información solicitada, enviaran al Oficial de Protección de Datos Personales y/o al Responsable de la Unidad de Transparencia la información.

3. Con la información enviada por las áreas al Oficial de Protección de Datos Personales y/o al Responsable de la Unidad de Transparencia, se procederá a integrar la información tomando en cuenta el Punto III. Elementos que debe contener el Documento de Seguridad.

4. Integrado el Documento de Seguridad, el Oficial de Protección de Datos Personales y/o al Responsable de la Unidad de Transparencia, deberá remitir el Documento de Seguridad al Comité de Transparencia para su revisión y aprobación.

5. Aprobado el Documento de Seguridad, se deberá publicar en el portal institucional del sujeto obligado.

6. GLOSARIO

Activos	Todo elemento de valor para una organización, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documento de papel.
Activos críticos	Activos que un responsable considera como lo más valiosos y que, si ocurre su pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizada, podría provocar una crisis, y comprometer las operaciones, la prestación de servicios o incluso la existencia de la organización.
Confidencialidad	Propiedad de la información para evitar su acceso, divulgación o revelación no autorizados.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
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, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
Administrador	Servidora o servidor público o persona física facultada y nombrada por el responsable para llevar a cabo tratamiento de datos personales y que tiene bajo su responsabilidad los sistemas y bases de datos personales.

Disponibilidad	Propiedad de la información para ser accesible y utilizable cuando se requiera.
Encargado	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.
Integridad	Propiedad de la información para salvaguardar la exactitud y completitud de la información.
Riesgo	Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que este cause un impacto negativo o daño.
Responsable	Los sujetos obligados del ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo del Poder Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos público. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal serán responsables de conformidad con la normatividad aplicable para la protección de datos personales.
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.

Vulnerabilidad	Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.
Vulneración de seguridad	Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento.
Usuario	Servidor o servidora pública que utiliza, trata, procesa, conserva, elimina los datos personales que se recaban de acuerdo a cada finalidad.

7. Normatividad

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado Libre y Soberano del Estado de Oaxaca.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.
- Ley General de Archivos.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público. INAI.
- Lineamientos Generales de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

En cumplimiento con lo establecido en el artículo 15 fracción IX inciso g) del Reglamento Interno del Órgano Garante de Acceso a la Información Pública, Transparencia, Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca, la Guía para Sujetos Obligados Elaboración del Documento de Seguridad, fue elaborada por el Departamento Protección de Datos Personales y Archivo; y aprobada por el Consejo General del Órgano Garante, mediante la Décima Cuarta Sesión Ordinaria celebrada el trece de julio del dos mil veintidós.