DOCUMENTO DE SEGURIDAD

DIRECCIÓN GENERAL DE POBLACIÓN
DE OAXACA

Edificio “G”, “María Sabina” (Planta Baja), Ala Izquierda Centro Administrativo del Poder Ejecutivo y Judicial General Porfirio Díaz, “Soldado de la Patria” Reyes Mantecón, San Bartolo Coyotepec, CP 71294
Tel. Conmutador.: 01 (951) 50 16900 Ext.26133

PRESENTACIÓN

La definición básica de datos personales dice que es información concerniente a una persona física, con la cual puede ser identificada o identificable. Dentro de los datos personales hay una categoría que se denomina “datos personales sensibles”, que requieren especial protección, ya que refieren a información que afecta a la esfera más íntima de una persona o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave, como la información genética, el estado de salud presente y futuro, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, origen racial o étnico y preferencia sexual.

El artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

La Dirección General de Población de Oaxaca en su carácter de sujeto obligado, entre los deberes, conforme a los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el 27 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca, está el de elaborar el presente Documento de Seguridad.

El Documento de Seguridad es el 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.

CONTENIDO

1. INVENTARIO DE LOS DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

1.1 formas de obtención de los datos personales.

ÁREA	MEDIO DE RECOLECCIÓN
Dirección General	• Formatos físicos • Formatos electrónicos
Asesor y Unidad de Transparencia	• Formatos físicos • Formatos electrónicos
Departamento Administrativo	• Formatos físicos • Carpetas electrónicas
Departamento de Informática	• Formatos físicos • Formatos electrónicos
Departamento de Educación y Comunicación en Población	• Formatos físicos • Formatos electrónicos
Departamento de Migración y Medio Ambiente	• Formatos electrónicos
Departamento de Investigación en Población.	• Formatos físicos • Formatos electrónicos

1.2 Finalidades de cada tratamiento de datos personales.

ÁREA	FINALIDADES DEL TRATAMIENTO
Dirección General	° Recabar datos de las y los participantes de las diferentes actividades que realiza la Dirección a través de internet. ° Recabar datos de las y los asistentes a las reuniones de trabajo con el Titular de la Dirección. ° Recabar información de los acuerdos tomados de las sesiones del equipo de trabajo que conforma la Dirección.
Asesor y Unidad de Transparencia	° Registro de los integrantes y asistentes de cada una de las sesiones programadas del Consejo de Administración y del Comité de Transparencia.
Departamento Administrativo	° Integración del expediente personal. ° Generación de contratos y nombramientos. ° Administrar asistencia y puntualidad del personal que labora en la Dirección. ° Administrar nómina y prestaciones. ° Registro y alta ante el Instituto Mexicano del Seguro Social. ° Elaboración de contratos y comprobantes fiscales por concepto de pagos a proveedores y servicios contratados.
Departamento de Informática	° Referencias para respuestas a solicitudes de información. ° Evidencia de entrega de información sociodemográfica a municipios del estado de Oaxaca.
Departamento de Educación y Comunicación en Población	° Registro de asistencia a reuniones de trabajo. ° Procedimiento de participación en el certamen de dibujo infantil y juvenil.
Departamento de Migración y Medio Ambiente	° Administración de la información de los autores que participan en las ediciones de la revista Oaxaca Población Siglo XXI.
Departamento de Investigación en Población.	° Referencias para respuestas a solicitudes de información.

1.3 Tipos de datos personales que se tratan y si son sensibles.

ÁREA	TIPOS DE DATOS PERSONALES	SENSIBLES
Dirección General	• Nombre • Correo electrónico • Edad	
Asesor y Unidad de Transparencia	• Nombre • Teléfono particular • Teléfono celular • Correo electrónico • Firma autógrafa • Puesto o cargo que desempeña • Domicilio de trabajo • Correo electrónico institucional • Teléfono institucional • Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)	
Departamento Administrativo	• 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 • Edad • Fotografía • Referencias personales • Estatura • Peso • Tipo de sangre • 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 • Trayectoria educativa • Títulos • Cédula profesional • Certificados • Ingresos • Cuentas bancarias • Seguros • Pasatiempos • Deportes que practica • Estado de salud físico presente, pasado o futuro	Sí
Departamento de Informática	• Nombre • Correo electrónico • Firma autógrafa • Puesto o cargo que desempeña • Correo electrónico institucional • Teléfono institucional	
Departamento de Educación y Comunicación en Población	• Nombre • Lugar de nacimiento • Teléfono particular • Teléfono celular • Correo electrónico • Edad • Puesto o cargo que desempeña • Domicilio de trabajo • Correo electrónico institucional • Teléfono institucional • Trayectoria educativa	
Departamento de Migración y Medio Ambiente	• Nombre • Teléfono particular • Teléfono celular • Correo electrónico • Firma autógrafa • Puesto o cargo que desempeña • Correo electrónico institucional • Teléfono institucional • Títulos	

Departamento de Investigación en Población.	• Nombre • Teléfono celular • Correo electrónico • Puesto o cargo que desempeña • Domicilio de trabajo • Correo electrónico institucional • Teléfono institucional	

1.4 Nuevas medidas de seguridad.

ÁREA	MEDIDAS DE SEGURIDAD A IMPLEMENTAR	TIPO DE MEDIDA DE SEGURIDAD
Dirección General	Tener bajo llave la información. Registro en bitácora de los solicitantes de la información. Autorización del titular para dar acceso a las carpetas digitales.	- Física - Física - Técnica
Asesor y Unidad de Transparencia	Colocar el aviso “Solo personal autorizado”. Registro en bitácora de los solicitantes de la información.	- Física - Física
Departamento Administrativo	Colocar el aviso “Solo personal autorizado”.	- Física
Departamento de Informática	Colocar el aviso “Solo personal autorizado”.	- Física
Departamento de Educación y Comunicación en Población	Colocar el aviso “Solo personal autorizado”. Registro en bitácora de los solicitantes de la información.	- Física - Física
Departamento de Migración y Medio Ambiente	Guardar los archivos bajo contraseña.	- Técnica

Departamento de Investigación en Población.	Guardar los archivos bajo contraseña. Guardar en una caja negra las solicitudes de información que lleguen de manera física.	- Técnica - Física

2.- CICLO DE VIDA DE LOS DATOS PERSONALES

Las actividades consideradas dentro del ciclo de vida de los datos personales son:

Obtención: La obtención de datos personales comprende todas las tareas en donde los datos personales son creados de manera directa por fuentes autorizadas o en forma indirecta a través de transferencias o generados mediante procedimientos de deducción.

Almacenamiento: Es el proceso por medio del cual se guardan los datos personales en forma electrónica, impresa o cualquier otro medio.

Uso: El uso de los datos personales implica el acceso, manejo y procesamiento para el propósito que fueron creados.

Divulgación: La divulgación consiste en las remisiones y transferencias de los datos personales hacia otras instancias que requieren y tienen autorización para el tratamiento de los datos personales.

Bloqueo: El bloqueo se realiza cuando los datos personales ya no son de utilidad, pero por alguna disposición regulatoria interna o externa deben retenerse.

Cancelación: La cancelación o destrucción de los datos personales implica la eliminación de la información cuando deja de ser útil para el propósito que fue creada.

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 considerar.

ÁREA	PERIODO DE CONSERVACIÓN
Dirección General	5 años
Asesor y Unidad de Transparencia	5 años
Departamento Administrativo	Permanente
Departamento de Informática	5 años
Departamento de Educación y Comunicación en Población	5 años
Departamento de Migración y Medio Ambiente	5 años
Departamento de Investigación en Población.	3 años

3.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN LOS DATOS PERSONALES.

En todos los procesos donde se tratan datos personales se identifican los roles y responsabilidades de las personas que tienen acceso a los datos, para ello se crea una matriz de responsabilidades en donde se especifica, para cada dato personal, qué perfil tiene acceso a los datos y con qué nivel de privilegio.

ÁREA	ADMINISTRADOR	OPERADOR	FUNCIONES
Dirección General	Carlos Alberto Holder Gómez	Aurelia Monserrat Salinas Vásquez	Fungir como enlace de comunicación con las dependencias y entidades de la administración pública estatal.
Asesor y Unidad de Transparencia	Ayrton Adrián Fierro Reyes	Gabriela Vanessa Rodríguez Valtierra	Revisar, integrar, mantener, concertar y establecer las condiciones con los integrantes de las actas de sesiones del Consejo de Administración y del Comité de Transparencia, llevar la asistencia y registro de los integrantes y participantes el día de la sesión. Establecidas en el artículo 8 del Reglamento Interno de la Dirección.
Departamento Administrativo	Gloria Antonio Ordáz	Laura Vásquez Jiménez	Actualización del archivo de los expedientes personales de los servidores públicos de la DIGEPO. Reglamento Interno de la DIGEPO, Artículo 10 fracción II.
Departamento de Informática	Raziel Ventura Cruz	Raziel Ventura Cruz	Resguardo y referencia para respuestas por el medio de entrega requerido: impreso o digital en el formato que mejor convenga al interesado.
Departamento de Educación y Comunicación en Población	Andrea Aguilar Cruz	Andrea Aguilar Cruz	Revisar, integrar, mantener y concertar reuniones de sesiones ordinarias y de trabajo del Grupo Estatal de Prevención del Embarazo en Adolescentes en Oaxaca. Llevar la asistencia y registro de los integrantes y participantes de dichas sesiones. Coordinar la fase estatal del Concurso Nacional de Dibujo Infantil y Juvenil, implica la

			recepción de las obras de manera física y la sistematización de datos de los concursantes, como edad, nombre, grado escolar, dirección, contacto y título de obra.
Departamento de Migración y Medio Ambiente	Aleida Escamilla Ramírez	Aleida Escamilla Ramírez	Revisar, integrar y concentrar la información de los autores que participan en las distintas ediciones de la revista Oaxaca Población Siglo XXI.
Departamento de Investigación en Población.	Lenin Alexis García Vargas	Lenin Alexis García Vargas	Revisar, integrar y actualizar la información de las solicitudes de información al departamento de investigación en la base de datos.

4.- ANÁLISIS DE RIESGOS

Tanto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 33 fracción IV y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca en su artículo 26 fracción IV, establecen que se debe contar con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento como pueden ser, de manera enunciativa mas no limitativa: hardware, software, personal del responsable, entre otros.

El responsable de esta actividad deberá considerar 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 los datos personales y las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Los beneficios de contar con un análisis de riesgos son grandes y algunos de ellos son: soporte a decisiones estratégicas, apoyo en la definición y asignación efectiva de recursos, justificar esfuerzos en tiempo, recurso humano y financieros, promover la mejora continua y transmitir confianza a empleados.

Para determinar las medidas de seguridad a implementar se analizaron 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 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).

NÚMERO DE TITULARES

ÁREA	NÚMERO DE TITULARES
Dirección General	250
Asesor y Unidad de Transparencia	35
Departamento Administrativo	23
Departamento de Informática	1
Departamento de Educación y Comunicación en Población	344
Departamento de Migración y Medio Ambiente	26
Departamento de Investigación en Población.	20
TOTAL	**699**

Identificación y clasificación de los datos personales

- **Datos con riesgo inherente bajo:** Se considera información general concerniente a una persona física identificada o identificable, como: datos de identificación, información académica o laboral.
- **Datos con riesgo inherente medio:** Se contemplan datos que permitan conocer la ubicación física de la persona, como: dirección física, información relativa al transito de las personas dentro y fuera del país, así como, número de dependientes, beneficiarios, familiares, referencias laborales y referencias personales.
- **Datos con riesgo inherente alto:** Se contemplan los datos personales sensibles, aquellos 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.
- **Datos con riesgo inherente reforzado:** Son aquellos como: información adicional de tarjeta bancaria (número de tarjeta de crédito y/o débito combinado con cualquier otro contenido de la misma como fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (NIP).

Identificación de tipo de datos y de nivel de riesgo inherente

TIPO DE DATO	NIVEL DE RIESGO INHERENTE
Ubicación en conjunto con patrimoniales	REFORZADO
Información adicional de tarjeta bancaria	REFORZADO
Titulares de alto riesgo	REFORZADO
Salud	ALTO
Origen, creencias e ideológicos	ALTO
Ubicación	MEDIO
Patrimoniales	MEDIO
Autenticación	MEDIO
Jurídicos	MEDIO
Tarjeta bancaria	MEDIO
Personales de identificación	BAJO

Considerando lo anterior, el número de titulares es de 679 de los cuales no recabamos datos sensibles que pudieran afectar a la esfera más íntima de una persona o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave, el nivel de riesgo inherente de los datos personales tratados por las distintas áreas que los recaban es:

NIVEL DE RIESGO INHERENTE MEDIO

5.- ANÁLISIS DE BRECHA

En cumplimiento al artículo 33 fracción V de la Ley General, que establece realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

El análisis de brecha consiste en determinar la diferencia entre las medidas de seguridad existentes y las que faltan para reducir el riesgo hasta un nivel por abajo del establecido por la organización como nivel aceptable.

5.1. Medidas de seguridad existentes y efectivas

ÁREA	MEDIDAS DE SEGURIDAD EXISTENTES
Dirección General	Se resguardan los expedientes en un archivero de lámina de tres cajones, con número de inventario SICIPO 803987, el cual permanece bajo llave. Los documentos electrónicos se encuentran en el drive de DIGEPO bajo contraseña.
Asesor y Unidad de Transparencia	Se resguardan los expedientes en un archivero de lámina de tres cajones, con número de inventario SICIPO 806785, el cual permanece bajo llave. Los archivos electrónicos se encuentran organizados en carpetas en la PC del área de Asesor.
Departamento Administrativo	Los expedientes se resguardan en el primer cajón de un archivero gris de lámina en el área de recursos humanos, el cual permanece bajo llave.

Departamento de Informática	Se resguardan los expedientes en una caja de archivo estándar en el área designada para el Departamento de Informática
Departamento de Educación y Comunicación en Población	Se resguardan los expedientes en un archivero con clasificación por carpetas y se cierra la oficina con llave.
Departamento de Migración y Medio Ambiente	Se resguardan las reseñas en la PC del Departamento de Migración y Medio Ambiente a la cual solamente tiene acceso la persona responsable de la información.
Departamento de Investigación en Población.	La base de datos de resguarda de manera electrónica en un archivo drive, y además en una memoria USB.

5.2. Medidas de seguridad a implementar

MEDIDAS DE SEGURIDAD A IMPLEMENTAR	TIPO DE MEDIDA
1.- Roles y responsabilidades: Identificar y definir los roles y responsabilidades de las personas que tienen acceso a los datos personales, qué perfil y con que nivel de privilegio según sus facultades.	Administrativa
2.- Seguridad en la transferencia o remisión: En caso de contar con la figura de encargado, contar con el documento que avale la transferencia y que contenga una cláusula de confidencialidad de la información.	Administrativa
3.- Inventario de activos: Identificar los activos y mantener actualizado el inventario de los mismos.	Física
4.- Controles de seguridad: Cada activo deberá contar con llave y un administrador que garantice la seguridad de la información.	Física
5.- Colocar aviso de "solo personal autorizado".	Física

6.- Registro en bitácora de los solicitantes de la información.	Física
7. Sensibilización y capacitación: Fomentar la cultura de la seguridad de la información, para ello, todos los servidores públicos de la Dirección deberán recibir capacitación de manera periódica respecto al tratamiento que realicen de los datos personales.	Administrativa
8.- Eliminación de los derechos de acceso: Los derechos de acceso de los servidores públicos responsables y encargados a las instalaciones o al tratamiento de la información, deben ser removidos en cuanto termine la relación laboral o de servicios, o en caso de realizar ajustes a las funciones del servidor público o encargado.	Administrativa
9.- Establecer contraseñas: Implementar contraseñas para toda la información que se tiene resguardada en equipos de cómputo y medios de almacenamiento electrónico.	Técnica
10.- Eliminación de forma segura de información: Establecer mecanismos para eliminar de manera segura información tanto en equipos de cómputo como elementos físicos, tomando precauciones con los procedimientos de reutilización.	Física

6.- PLAN DE TRABAJO

El plan de trabajo es parte medular del documento de seguridad y es donde se detallan las acciones tomadas para implementar las medidas de seguridad.

En cumplimiento a los establecido en el artículo 33 fracción VI de la Ley General, ayudados del análisis de riesgos y el análisis de brecha, se seleccionaron las medidas de seguridad aplicables a la protección de datos personales. La implementación de cada uno de los mecanismos de seguridad se realizará de acuerdo al siguiente plan de trabajo:

ACCIONES A IMPLEMENTAR	ENE	FEB	MAR	ABRIL	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1.- Roles y responsabilidades:												

Identificar y definir los roles y responsabilidades de las personas que tienen acceso a los datos personales.												
2.- Seguridad en la transferencia o remisión.												
3.- Inventario de activos: Identificar los activos y mantener actualizado el inventario de los mismos.												
4.- Controles de seguridad: Cada activo deberá contar con llave y un administrador.												
5.- Colocar aviso de "solo personal autorizado".												
6.- Registro en bitácora de los solicitantes de la información.												
7. Sensibilización y capacitación: Capacitación de manera periódica respecto al tratamiento de los datos personales.												
8.- Eliminación de los derechos de acceso: Remover los derechos en cuanto termine la relación laboral.												
9.- Establecer contraseñas: Para toda la información que se tiene resguardada en equipos de												

cómputo y medios de almacenamiento electrónico.												
10.- Eliminación de forma segura de información: Establecer mecanismos para eliminar de manera segura información												

7.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

En términos de lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo 33 fracción VII, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Con base en el Plan de Trabajo planteado se evaluarán de manera semestral en los meses de julio y diciembre, tanto las medidas administrativas, físicas y técnicas, así también se trabajará con los responsables de las unidades administrativas para revisar la efectividad de las medidas de seguridad implementadas, informando los avances en las sesiones del Comité de Transparencia.

MECANISMO DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	ENE	FEB	MAR	ABRIL	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Visita a las áreas para verificación de las medidas administrativas, físicas y técnicas												
Evaluación de la efectividad de las medidas de seguridad.												

8.- PROGRAMA GENERAL DE CAPACITACIÓN

La mejor medida de seguridad contra posibles vulneraciones es contar con servidores públicos conscientes de sus deberes respecto a la protección de datos personales, que identifiquen sus atribuciones, facultades y funciones para su adecuado tratamiento.

Los Lineamientos Generales de Protección de Datos Personales establecen que el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a 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.

El presente Programa se sustenta en los temas y acciones de capacitación del Departamento de Formación y Capacitación, dependiente de la Dirección de Comunicación, Capacitación, Evaluación, Archivo y Datos Personales del Instituto de Acceso a la Información Pública y Protección de Datos Personales de Oaxaca.

TEMAS PARA CAPACITACIÓN	ENE	FEB	MAR	ABRIL	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Funciones de las áreas administrativas												
Formas y medios para publicar información												
Versiones públicas												
Obligaciones en materia de datos personales												
Documento de Seguridad												