IAIP.

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

DOCUMENTO DE SEGURIDAD.

Instituto de Acceso a la Informaci ó n P ú blica y Protecci ó n de Datos Personales del Estado de Oaxaca.

PRESENTACIÓN

El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de Oaxaca (IAIP), ejerce dos funciones: como Órgano garante y como Sujeto obligado; en su rol de Sujeto obligado debe garantizar el debido tratamiento de los datos personales que obran en su poder; por lo tanto es indispensable cumplir con el ***PRINCIPIO DE RESPONSABILIDAD*** establecido en el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDP) y en el artículo 9 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca (LPDPO).

Para dar cumplimiento a este principio deberá elaborar el Documento de Seguridad, de acuerdo al artículo 34 de la LGPDP y el artículo 27 de la LPDPO, este documento debe contener las medidas de seguridad establecidas al interior del Sujeto obligado.

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.

CONTENIDO

1. El inventario de datos personales y de los sistemas de tratamiento.

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

1.2. Finalidades de cada tratamiento de datos personales.

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

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

2. Ciclo de vida de los datos personales.
3. Las funciones y obligaciones de las personas que tratan datos personales.
4. El análisis de riesgos.
5. El análisis de brecha.
6. El plan de trabajo.
7. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
8. El programa de capacitación.
9. Glosario.
10. Normatividad.
11. Participantes.

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

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

Área	Medio de recolección
Departamento de Recursos Financieros	▪ Formatos físicos
Departamento de Recursos Materiales	
Departamento de Recursos Humanos	
Dirección de Asuntos Jurídicos	▪ Formatos físicos ▪ Carpetas electrónicas
Departamento de Formación y Capacitación	▪ Formatos físicos ▪ Formatos electrónicos
Dirección de Gobierno Abierto	▪ Formatos Físicos ▪ Vía telefónica ▪ Formulario electrónico

1.2. FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES

Área	Finalidades del tratamiento
Departamento de Recursos Humanos	• Procedimiento de selección e integración de expediente del personal. • Elaboración de sus respectivos contratos, nombramientos • Comprobantes fiscales por concepto de percepciones y deducciones (CFDI). • Registro y control de asistencias del personal que labora en el Instituto, para trámite de su tarjeta bancaria. • Registro y alta ante el Instituto Mexicano del Seguro Social, publicación de información curricular, así como enviarles convocatoria para las capacitaciones, cursos y diplomados convocados por el órgano garante. • Implementar políticas de control interno para el funcionamiento interior del Instituto.
Departamento de Recursos Financieros	• Pago y comprobación de servicios del proveedor o trabajador.
Departamento de Recursos Materiales	• Procedimiento de selección, y elaboración de contratos, comprobantes fiscales por concepto de pagos a proveedores y servicios contratados
Departamento de Formación y Capacitación	▪ Trámite a Solicitud de Capacitación ▪ Registro de asistentes a capacitación, eventos, talleres, conferencias, generar estadísticas e informes. ▪ Generar constancias.
Dirección de Gobierno Abierto	▪ Asistencia a sesiones, eventos, charlas, conferencias, ▪ Enviar información de los eventos del IAIP. ▪ Participación en convocatorias
Dirección de Asuntos Jurídicos	▪ Contar con un registro de las asesorías brindadas a los sujetos obligados. ▪ Contar con un registro de reuniones de trabajo. ▪ Trámite y substanciación de denuncias administrativas y penales. ▪ Documentar la firma de convenios y contratos.

1.3. CATÁLOGO DE LOS TIPOS DE DATOS PERSONALES QUE SE TRATAN Y SI SON SENSIBLES.

Área	Tipos de datos personales	Sensibles
Recursos Humanos	• Identificación • Datos Patrimoniales • De Salud • Biométricos • Características físicas • Académicos • Laborales	✓
Recursos Financieros	• Identificación	x
Recursos Materiales	• Identificación • Patrimoniales	x
Formación y Capacitación	• De identificación • Laborales	✓
Dirección de Asuntos Jurídicos	• De identificación	x
Dirección de Gobierno Abierto	• De identificación	x

1.4. EXISTENCIA DE NUEVAS MEDIDAS DE SEGURIDAD QUE PUDIERAN REEMPLAZAR A UNO O MÁS CONTROLES IMPLEMENTADOS.

ELIMINADO: Cuatro párrafos, uno de siete renglones, uno de seis renglones y dos de cinco renglones. Fundamento Legal: artículos 116 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 2 fracción IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 6 fracción III, VII, XVIII, XXXIII, 56 y 57 fracción I de la ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca y, 3 fracción VIII, 5 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; artículo 9 fracción XIV Reglamento Interno del Instituto de Acceso a la Información Pública y Protección de Datos Personales. Por tratarse de información que da cuenta de las medidas de seguridad respecto al tratamiento y conservación de los datos personales que se recaban.

ELIMINADO: Tres párrafos, uno de dos renglones, uno de diez renglones y uno de seis renglones. Fundamento Legal: artículos 116 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 2 fracción IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 6 fracción III, VII, XVIII, XXXIII, 56 y 57 fracción I de la ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca y, 3 fracción VIII, 5 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; artículo 9 fracción XIV Reglamento Interno del Instituto de Acceso a la Información Pública y Protección de Datos Personales. Por tratarse de información que da cuenta de las medidas de seguridad respecto al tratamiento y conservación de los datos personales que se recaban.

Área	Medidas de seguridad a implementar	Tipo de Medida de Seguridad
Departamento de Recursos Humanos	▪ Colocar aviso de "solo personal autorizado"	▪ Física
Departamento de Recursos Financieros	▪ Registro en bitácora de los solicitantes de la información. ▪ Señalar en un listado las personas que tienen acceso a los soportes electrónicos del sistema.	▪ Física
Departamento de Recursos Materiales	▪ Registro en bitácora de los solicitantes de la información. ▪ Señalar en un listado las personas que tienen acceso a los soportes electrónicos del sistema.	▪ Física
Dirección de Asuntos Jurídicos	▪ Contar con más archiveros	▪ Física
Dirección de Gobierno Abierto	▪ Resguardar los expedientes en un archivero metálico ▪ Crear un respaldo en un disco duro de los archivos físico y digitales que contienen datos personales. ▪ Definir el tiempo de conservación acorde a las finalidades para las que se recaban los datos personales.	▪ Física

2. 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 considerar.

Área	Periodo de conservación
Departamento de Recursos Humanos	De acuerdo a lo establecido en la Norma de Archivo Contable Gubernamental NACG 01 Disposiciones Aplicables Al Archivo Contable Gubernamental el ciclo de vida son de 5 años salvo excepciones con fundamento en los artículos 67 según sea el caso de 10 años
Departamento de Recursos Financieros	
Departamento de Recursos Materiales	
Dirección de Asuntos Jurídicos	01 año
Departamento de Quejas y Denuncias	05 años
Departamento de Formación y Capacitación	05 años
Dirección de Gobierno Abierto	02 años – Registros de asistencia físicos. 01 año - Registros recabados vía telefónica. Durante la vigencia de la convocatoria- Formulario electrónico.

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

Establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al **sistema de gestión implementado**.

ÁREA	ADMINISTRADOR	OPERADOR	FUNCIONES
Dirección de Comunicación, Capacitación, Evaluación, Archivo y Datos Personales.			1.Promover, difundir y desarrollar foros, seminarios, talleres, eventos y actividades relacionadas con la cultura de la transparencia, acceso a la información pública, protección de datos personales, gobierno abierto, rendición de cuentas, combate a la corrupción, participación ciudadana, accesibilidad e innovación tecnológica, y organización y conservación de archivos; y difundir la realización de eventos similares a nivel nacional e internacional. Artículo 12. Reglamento Interno .IAIP
Departamento de Capacitación	Emilia López Morales	Persilia Calvo Ramírez	1. Capacitar y asesorar a los Sujetos obligados en la operación de los Sistemas que integran la PNT. 2. Promover y en su caso, convocar, planear, coordinar y ejecutar la capacitación, asesoría y actualización permanente de los servidores públicos del Instituto, de los Sujetos obligados y de la Sociedad civil en las materias de transparencia, gobierno abierto, rendición de cuentas, combate a la corrupción, participación ciudadana, accesibilidad e innovación tecnológica, archivos, acceso a la información pública y protección de datos personales. Manual de Organización. IAIP.
Departamento de Gobierno Abierto	Rafael García Leyva	Arantxa Sánchez López	1. Asesorar a los sujetos obligados, instituciones, organizaciones públicas y organizaciones de la sociedad civil, para propiciar el diseño, conceptualización, desarrollo y construcción de políticas públicas de gobierno abierto; 2. Coordinar las acciones y actividades del Secretariado Técnico de Gobierno Abierto del Estado de Oaxaca para el correcto cumplimiento del Plan de Acción Local; 3.Establecer y mantener contacto con la sociedad civil organizada y con los sujetos obligados para conciliar el acercamiento necesario para la construcción de políticas públicas de transparencia y Gobierno Abierto, para la solución de problemas públicos. Artículo 16. Reglamento Interno.IAIP.

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

ÁREA	ADMINISTRADOR	OPERADOR	FUNCIONES
Dirección Jurídica	Lic. Ricardo Dorantes Jiménez		Establecidas en el artículo 14 del Reglamento interno del Instituto
Departamento de Quejas y Denuncias		Thomas Aguilar Mendoza	Establecidas en el Manual de Organización
Dirección de Administración	Lic. Lauro Alonzo Martínez.		1.Proponer al Consejo General y ejecutar las políticas generales, criterios técnicos y lineamientos para la administración eficaz y eficiente de los recursos humanos y materiales; así como la planeación, administración presupuestal, financiera y contable del Instituto; 2. Coordinar y elaborar los proyectos del Plan de Trabajo Institucional, Presupuesto Anual de Ingresos y Egresos, y Programa Operativo Anual del Instituto, para aprobación del Consejo General. Artículo 15. Reglamento Interno. IAIP
Recursos Humanos		Citlally Ruiz Vásquez	1. Gestionar la autorización y apoyar en la supervisión de las acciones relacionadas con la selección y contratación, pago de remuneraciones, prestaciones, altas, bajas, licencias y todo tipo de movimientos de personal que se tramiten, apegándose a las políticas establecidas. 2. Elaborar los contratos e integrar los documentos requeridos para la dotación de personal al servicio del Instituto, en términos de lo que establece la Ley en la materia. 3. Realizar el trámite de los nombramientos de mandos medios y superiores de acuerdo a la estructura orgánica autorizada, verificando que se integren los expedientes correspondientes. 4. Generar el registro del personal ante el Instituto Mexicano del Seguro Social, a través del Sistema Único de Autodeterminación, cada vez que los movimientos del personal así lo requieran. 5. Controlar la asistencia del personal a sus labores y registrar las incidencias que derivado de ello se generen. 6. Elaborar el cálculo de la nómina, los recibos y los Comprobantes Fiscales Digitales, para el pago de las remuneraciones al personal que labore en el Instituto. 7. Generar el control y comprobación de la ministración del recurso enviado por la Secretaría de Finanzas para el pago de la nómina por remuneraciones al personal del Instituto 8.Identificar las necesidades de capacitación del personal al servicio del Instituto. Manual de Organización IAIP.

ÁREA	ADMINISTRADOR	OPERADOR	FUNCIONES
Departamento de Recursos Financieros	Lic. Lauro Alonzo Martínez	▪ Tonatiuh Valdez Pérez ▪ Iriana Martínez López.	1. Implementar e informar el proceso de recepción y pago de facturas, recibos o documentos de cobro a favor de proveedores y prestadores de servicios. 2. Realizar la integración de los expedientes con la documentación justificativa y comprobatoria, así como de las operaciones financieras que se realicen y que ampare el ejercicio presupuestal de los recursos autorizados al Instituto. 3. Asegurar el adecuado registro, archivo y resguardo de los expedientes y de la documentación justificativa y comprobatoria de las operaciones financieras y del ejercicio presupuestal de los recursos autorizados al instituto, para facilitar las acciones de consulta y verificación. 4. Generar y actualizar la información necesaria para la óptima operación del SIPOT. Manual de Organización. IAIP.
Departamento de Recursos Materiales		Nelly Gisela Guerrero Lascares	10. Verificar la correcta elaboración e integración de los contratos, convenios y demás documentos relacionados con la adquisición, arrendamiento y contratación de bienes y servicios suministrados al Instituto. 15. Coadyuvar en la contratación, operación y control de los servicios generales.16. Otorgar seguimiento a las solicitudes de información que requieran los Órganos de Control internos, externos y de Fiscalización en materia de recursos humanos, materiales y financieros del Instituto. Manual de organización.IAIP.

4. ANÁLISIS DE RIESGOS

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 a 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 analizaron los siguientes puntos:

a) **Beneficio para el atacante:** Aquellos datos personales que representen mayor beneficio tienen mas 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 mas probabilidad de ser atacados. (internet es un medio mas anónimo que presentarse físicamente a las instalaciones de la institución)

Número de Titulares

ÁREA	NÚMERO DE TITULARES
Recursos Humanos	
Recursos Financieros	95
Recursos Materiales	
Dirección de Asuntos Jurídicos	
Quejas y denuncias	50
Formación y Capacitación	2500
Dirección de Gobierno Abierto	250
TOTAL	2,895 titulares

Identificación y clasificación de 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 a 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 debito combinado con cualquier otro contenido de la misma como fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN)

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

Tomando en cuenta lo anterior y que no pertenecemos a un sector especifico, no asignamos valor a los datos personales que se manejan y que el ciclo de vida de estos no está del todo determinado; aunque el número de titulares es de 2,895 no recabamos datos sensibles o que pudieran afectar la esfera más intima de los titulares; 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

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.

ELIMINADO: Cuatro párrafos, uno de siete renglones, uno de seis renglones y dos de cinco renglones. Fundamento Legal: artículos 116 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 2 fracción IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 6 fracción III, VII, XVIII, XXXIII, 56 y 57 fracción I de la ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca y, 3 fracción VIII, 5 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; artículo 9 fracción XIV Reglamento Interno del Instituto de Acceso a la Información Pública y Protección de Datos Personales. Por tratarse de información que da cuenta de las medidas de seguridad respecto al tratamiento y conservación de los datos personales que se recaban.

ELIMINADO: Cuatro párrafos, uno de siete renglones, uno de dos renglones, uno de cuatro renglones y uno de cuatro renglones. Fundamento Legal: artículos 116 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 2 fracción IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 6 fracción III, VII, XVIII, XXXIII, 56 y 57 fracción I de la ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca y, 3 fracción VIII, 5 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca; artículo 9 fracción XIV Reglamento Interno del Instituto de Acceso a la Información Pública y Protección de Datos Personales. Por tratarse de información que da cuenta de las medidas de seguridad respecto al tratamiento y conservación de los datos personales que se recaban.

5.2. 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 a Implementar	Tipo de Medida
1. **Inventario de activos:** Todos los activos deben ser claramente identificados y un inventario de los activos mas importantes debe ser elaborado y mantenido.	**Física**
2. **Roles y responsabilidades:** Los roles y responsabilidades de los servidores públicos deben estar definidos y documentados de acuerdo a sus facultades.	**Administrativa**
3. **Términos y condiciones de empleo:** Como parte de las funciones de cada servidor público, se deberá acordar o establecer los términos o condiciones de confidencialidad , de acuerdo al tratamiento y responsabilidad de los datos personales que obran en su poder.	**Administrativa**

Medidas a Implementar	Tipo de Medida
4. Sensibilización y capacitación: Todos los servidores públicos del Instituto deberán recibir capacitación de manera periódica de acuerdo al tratamiento que realicen de los datos personales.	**Administrativa**
5. 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 clausula de confidencialidad de la información	**Administrativa**
6. Establecer controles de seguridad. Todos los activos deberán contar con llave y un administrador del mismo, que garantice la seguridad de la información.	**Física**
8. Eliminación de los derechos de acceso: Los derechos de acceso de los servidores públicos o 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. Catálogo de Sistemas Electrónicos. Integrar el catálogo de los activos que contienen datos personales.	**Técnica**

6. PLAN DE TRABAJO

Derivado de 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 se propone el siguiente plan de trabajo:

Acciones a implementar	Abril	Mayo	Junio	Julio	Agos	Sept	Oct	Nov	Dic
Realizar un inventario de los activos mas importantes.									
Definir y actualizar los roles y responsabilidades de los servidores públicos de acuerdo a sus facultades.									
Establecer los términos o condiciones de confidencialidad de acuerdo a las funciones de cada servidor público.									
Realizar actividades de capacitación dirigida a los servidores públicos del Instituto de acuerdo al tratamiento que realicen de datos personales.									
Incorporar clausula de confidencialidad a los instrumentos jurídicos que avale la transferencia									

Acciones a implementar	Abril	Mayo	Junio	Julio	Agos	Sept	Oct	Nov	Dic
Todos los activos deberán contar con llave y un administrador del mismo, que garantice la seguridad de la información.									
Cancelar los derechos de acceso de los servidores públicos o 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.									
Catálogo de Sistemas Electrónicos. Integrar el catálogo de los activos que contienen datos personales.									

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

Las medidas de seguridad propuestas a implementar en cada una de las áreas del Instituto, se evaluaran de manera semestral, tanto las medidas de seguridad administrativas como las técnicas para determinar su eficacia o vulnerabilidad

Mecanismo de monitoreo y revisión de medidas de seguridad	**Abril**	**Mayo**	**Junio**	**Julio**	**Agos**	**Sept**	**Oct**	**Nov**	**Dic**
Visitas físicas a las áreas									
Revisión de las medidas de seguridad técnicas									

En las visitas físicas se revisara lo siguiente:

a) Nuevos activos que se incluyan en la gestión de riesgos.
b) Modificaciones necesarias a los activos , como podría ser el cambio o migración tecnológica.
c) Las nuevas amenazas que podrían estar activas dentro y fuera de su 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 aceptable de riesgo.
g) Los incidentes y vulneraciones de seguridad ocurridas.

8. PROGRAMA GENERAL DE CAPACITACIÓN.

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.

Temas para capacitación	Abril	Mayo	Junio	Julio	Agos	Sept	Oct	Nov	Dic
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca.									
Taller Respaldos de información									
Elaboración de versiones públicas									
Instrumentos internacionales en materia de protección de datos personales									
Declaraciones patrimonial y de intereses y acta de entrega recepción.									

9. 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 mas intima 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 el 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.

- **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.

10. NORMATIVIDAD.

- 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.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público. INAI.
- Reglamento Interno del Instituto De Acceso a la Información Pública y Protección de Datos Personales del Estado de Oaxaca
- Manual de Organización. Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de Oaxaca.
- Metodología de Análisis de Riesgo BAA. INAI.
- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales. INAI.

11. PARTICIPANTES.

- **Dirección de Administración**
  - Recursos Humanos
  - Recursos financieros
  - Recursos Materiales
- **Dirección de Asuntos Jurídicos**
  - Departamento de Quejas y Denuncias
- **Dirección de Gobierno Abierto**
- **Dirección de Tecnologías de Transparencia.**
- **Dirección de Comunicación, Capacitación, Evaluación, Archivo y Datos Personales**
  - Departamento de Formación y Capacitación.
  - Departamento de Datos Personales y Archivo.

En coordinación con la Oficial de Protección de Datos Personales del IAIP.

IAIP

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

www.iaipoaxaca.org.mx

IAIP Oaxaca | @IAIPOaxaca