TECNOLOGÍAS
AGENCIA DE TECNOLOGÍAS E INNOVACIÓN DIGITAL

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

El presente Documento de Seguridad se elabora con fundamento en los artículos 6°, apartado A, y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos; correlativos de la Constitución Política del Estado Libre y Soberano de Oaxaca; así como en los artículos 3, fracción XIV, 29 y 30, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, 2, 3, 11, 12, 13, 18, 19, 20, 26 al 43 y demás aplicables de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Oaxaca.

De manera específica, el artículo 33 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Oaxaca establece la obligación de las personas responsables de elaborar y mantener actualizado un Documento de seguridad.

En ese sentido, el presente instrumento documenta las acciones, controles y mecanismos implementados por la Agencia de Tecnologías e Innovación Digital para garantizar el adecuado tratamiento y protección de los datos personales bajo su posesión.

TECNOLOGÍAS
AGENCIA DE TECNOLOGÍAS E INNOVACIÓN DIGITAL

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA AGENCIA DE TECNOLOGÍAS E INNOVACIÓN DIGITAL

Contenido

Presentación

En el presente documento se establecen las medidas de seguridad administrativas, físicas y técnicas implementadas, con el propósito de garantizar la adecuada protección de los datos personales objeto de tratamiento por parte del personal responsable de su manejo, bajo la supervisión del Oficial de Protección de Datos Personales de la Agencia de Tecnologías e Innovación Digital, en ese sentido, el documento tiene como finalidad definir los mecanismos, controles, políticas, procedimientos y acciones orientadas a asegurar la confidencialidad, integridad y disponibilidad de los datos personales tratados por este sujeto obligado, así como prevenir su alteración, pérdida, transmisión, acceso o tratamiento no autorizado.

De igual forma, este documento establece un sistema de supervisión, vigilancia y mejora continua que permite verificar el cumplimiento de las políticas y medidas de protección de datos personales, así como identificar y mitigar riesgos derivados del tratamiento de la información. En ese sentido, y de conformidad con el artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable deberá actualizar el documento de seguridad.

Este Documento de Seguridad es de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier etapa del tratamiento de datos personales que se encuentren en posesión de la Agencia de Tecnologías e Innovación Digital, así como para toda persona física o moral, pública o privada, que con motivo de la prestación de un servicio, colaboración, convenio o relación contractual tenga acceso a dichos datos, de conformidad con lo establecido en la normatividad aplicable en materia de protección de datos personales.

De igual forma, el presente instrumento constituye una guía institucional para promover una cultura de protección de datos personales, responsabilidad administrativa y cumplimiento normativo dentro de la Agencia, fortaleciendo la confianza de la ciudadanía respecto del tratamiento legítimo, controlado e informado de su información personal.

Objetivo

Establecer las medidas de seguridad administrativas, físicas y técnicas, así como los mecanismos de control, supervisión y mejora continua aplicables al tratamiento de datos personales en posesión de la Agencia de Tecnologías e Innovación Digital, a fin de garantizar su protección conforme a los principios, deberes y obligaciones previstos en la normativa aplicable en materia de protección de datos personales, promoviendo criterios de actuación para las personas servidoras públicas y terceros autorizados que intervengan en dicho tratamiento, así como una cultura institucional basada en la legalidad, la responsabilidad, la rendición de cuentas y la protección del derecho humano a la privacidad.

Asimismo, el presente Documento de Seguridad tiene como finalidad definir las políticas, procedimientos y controles institucionales necesarios para prevenir el daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado de los datos personales, preservando su confidencialidad, integridad y disponibilidad mediante la implementación de medidas preventivas, correctivas y de gestión de riesgos.

Glosario

Agencia: A la Agencia de Tecnologías e Innovación Digital.

Áreas: Instancias del sujeto obligado previstas en el reglamento interno de la y Agencia de Tecnologías e Innovación Digital responsables o encargadas de los datos personales.

Confidencialidad: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados y que garantiza la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos 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 presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCOP: Los derechos de acceso, rectificación, cancelación, oposición y Portabilidad de datos personales.

Disponibilidad: Propiedad de la información para ser accesible y utilizable cuando se requiera.

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.

Inventario de datos personales: Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona identifica o identificable.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas, acciones y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información,

así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

Medidas de seguridad técnicas: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública. En este Documento se refiere a la Unidad de Transparencia a la que hace mención el artículo 30 del Reglamento Interno de la Agencia de Tecnologías e Innovación Digital.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

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.

Usuario: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones

por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

1. Inventario de datos personales y 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 Atención en Mesa (Mesa De Ayuda)	• Medios físicos • Medios electrónicos
Dirección Administrativa	• Medios físicos • Medios electrónicos
Dirección Jurídica	• Medios físicos • Medios electrónicos
Dirección de Desarrollo de Sistemas	• Medios electrónicos

Medios físicos: Documentos Físicos: (oficios, circulares, memorándums, solicitudes, registros, copias de documentos oficiales (identificaciones, actas, comprobantes) listas de asistencia, facturas, recibos, expedientes administrativos del personal, licencias, currículums, contratos, convenios, acuerdos firmados en papel, etc.
Medios electrónicos: Corre electrónico, bases de datos, páginas web, sitios web y dispositivos de almacenamiento (memoria USB, disco duro y CD).

1.2. Las finalidades de cada tratamiento de datos personales.

ÁREA	FINALIDAD DEL TRATAMIENTO
Departamento de Atención en Mesa (Mesa de ayuda)	1. Recibir, registrar, clasificar y canalizar solicitudes de servicio e incidencias tecnológicas mediante la Mesa de Ayuda. 2. Integrar y administrar tickets de atención en la plataforma institucional. 3. Dar seguimiento a solicitudes hasta su solución y cierre. 4. Establecer comunicación con personas usuarias internas y externas para atención de incidencias. 5. Escalar incidencias a niveles superiores

	conforme a la matriz de escalamiento. 6. Elaborar reportes semanales de actividades, incidencias atendidas y avances obtenidos. 7. Aplicar encuestas o mecanismos de satisfacción del usuario. 8. Resguardar evidencia documental y digital derivada de solicitudes de soporte.
Dirección Jurídica	1. Trámite y substanciación de solicitudes de acceso a la información, recursos de revisión y ejercicio de derechos ARCOP. 2. Creación de expedientes para establecer comunicación interinstitucional. 3. Elaboración de contratos, convenios y acuerdos de confidencialidad.
Dirección Administrativa	1. Integración de expedientes del personal. 2. Elaboración de altas y bajas de personal. 3. Registro de asistencia del personal que labora en la Entidad. 4. Publicación de información curricular. 5. Registro y elaboración de gafetes oficiales de personal. 6. Pago a personal que labora en la Entidad. 7. Pago y comprobación de servicios a proveedores. 8. Comprobación de viáticos. 9. Elaboración de contratos de adquisiciones. 10. Tramite de pago de servicios para el mantenimiento del edificio de la Entidad. 11. Elaboración de credenciales institucionales
Dirección de Desarrollo de Sistemas	1. Administrar y dar soporte a los sistemas

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

ÁREA	TIPOS DE DATOS PERSONALES	SENSIBLES
Departamento de Atención en Mesa (Mesa de ayuda)	• Identificación • Contacto • Laborales	
Dirección Jurídica	• Identificación • Contacto	

	• Laborales	
Dirección Administrativa	• Identificación • Contacto • Laborales • Salud • Académicos • Patrimoniales • Bancarios • Familiares	X
Dirección de Desarrollo de Sistemas	• Identificación • Contacto • Laborales	

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

ÁREA	MEDIDAS DE SEGURIDAD EXISTENTES
Departamento de Atención en Mesa (Mesa de ayuda)	Medida de seguridad de acceso a las instalaciones de esta Agencia, puerta con cerradura para acceso a la oficina, archiveros y cajones con llave, computadoras con usuarios y contraseñas, accesos a sistemas con usuarios y contraseñas.
Dirección Jurídica	Medidas de seguridad de acceso a las instalaciones de esta Agencia, archiveros y cajones con llave para el resguardo de documentos, avisos de privacidad, computadoras con usuarios y contraseñas, acceso a sistemas con usuario y contraseña (PNT, correos electrónicos, Sistema de ética e integridad y sistema de registro de entidades paraestatales).
Dirección Administrativa	Medida de seguridad de acceso a las instalaciones de esta Agencia, puerta con cerradura para acceso a la oficina, archiveros y cajones con llave, computadoras con usuarios y contraseñas, accesos a sistemas con usuarios y contraseñas.
Dirección de Desarrollo de Sistemas	Medida de seguridad que incluyen el uso de credenciales de acceso (usuarios y contraseñas) para computadoras y sistemas, gestión de accesos temporales mediante llaves o tokens, mecanismos de autenticación robusta, así como

	el registro de bitácoras de acceso y la supervisión continua, ya sea en tiempo real o de forma diferida, asimismo, se contempla la aplicación periódica de parches y actualizaciones de seguridad, junto con la implementación de soluciones de protección contra malware y mecanismos de defensa ante posibles ataques informáticos.

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.**

Área Administrativa	**Medidas de seguridad a implementar**	**Tipo de medida** (Administrativa, física o técnica)
Departamento de Atención en Mesa (Mesa de ayuda)	• Capacitaciones • Se recomienda establecer un espacio físico designado exclusivamente para el resguardo de documentos que contengan datos personales. Este lugar deberá contar con condiciones adecuadas de seguridad, tales como acceso restringido únicamente a personal autorizado, así como mecanismos de protección que garanticen la confidencialidad e integridad de la información almacenada. • Mantenimiento a equipos de cómputo y cambios periódicos de contraseñas	Administrativa Física Técnica
Dirección Jurídica	• Capacitaciones • Se recomienda establecer un espacio físico designado exclusivamente para el resguardo de documentos que	Administrativa

	contengan datos personales. Este lugar deberá contar con condiciones adecuadas de seguridad, tales como acceso restringido únicamente a personal autorizado, así como mecanismos de protección que garanticen la confidencialidad e integridad de la información almacenada. • Mantenimiento a equipos de cómputo y cambios periódicos de contraseñas	Física Técnica
Dirección Administrativa	• Capacitaciones • Se recomienda establecer un espacio físico designado exclusivamente para el resguardo de documentos que contengan datos personales. Este lugar deberá contar con condiciones adecuadas de seguridad, tales como acceso restringido únicamente a personal autorizado, así como mecanismos de protección que garanticen la confidencialidad e integridad de la información almacenada. • Mantenimiento a equipos de cómputo y cambios periódicos de contraseñas	Administrativa Física Técnica
Dirección de Desarrollo de Sistemas	• Capacitaciones • Se recomienda establecer un espacio físico designado exclusivamente para el resguardo de documentos que contengan datos personales. Este lugar deberá contar con condiciones adecuadas de seguridad, tales como acceso	Administrativa Física

	restringido únicamente a personal autorizado, así como mecanismos de protección que garanticen la confidencialidad e integridad de la información almacenada. • Mantenimiento a equipos de cómputo y cambios periódicos de contraseñas	Técnica

1.5. Ciclo de vida de los datos personales.

Tomando en consideración la obtención y el tratamiento de los datos personales que realiza la Agencia de Tecnologías e Innovación Digital, y de conformidad con la Ley General de Archivos y la normatividad en materia de protección de datos personales aplicable, se identifica el ciclo de vida de los datos personales contenidos en los documentos y expedientes que se generan, reciben y resguardan en el ejercicio de sus atribuciones.

Para tal efecto, se relacionan las finalidades del tratamiento con las series documentales, sus valores documentales y los plazos de conservación correspondientes, a fin de determinar el periodo durante el cual los datos personales permanecen en archivo de trámite y, en su caso, en archivo de concentración, hasta su destino final.

Lo anterior contribuye al adecuado resguardo, organización, conservación, control y disposición documental de los datos personales desde su obtención hasta la conclusión de su tratamiento.

Finalidades	Series documentales	Valores documentales	Plazos de conservación	
			Trámite	Concentración
Nóminas	En proceso	Administrativo, contable y legal.	2 años	3 años
Control de Correspondencia	En proceso	Administrativo	1 años	0 años
Certificaciones	En proceso	Administrativo	1 años	5 años
Servicios de	En proceso	Administrativ	1 años	5 años

Internet, Voz, Datos y Correos Electrónicos		o		
Construcción, Actualización y mantenimiento de portales institucionales	En proceso	Administrativo	1 años	5 años
Diseño e implementación de sistemas	En proceso	Administrativo	1 años	5 años
Soporte técnico de los sistemas de información	En proceso	Administrativo	1 años	5 años
Mantenimiento de equipo de computo	En proceso	Administrativo	1 años	5 años
Estadísticas	En proceso	Administrativo	1 años	5 años
Expedientes de Personal	En proceso	Administrativo	1 años	1 años
Altas y Bajas	En proceso	Administrativo y legal.	1 años	1 años
Recibos de pago	En proceso	Administrativo y legal.	1 años	1 años
Incidencias	En proceso	Administrativo y legal.	1 años	1 años
Estados Financieros	En proceso	Administrativo y Fiscal	1 años	5 años
Gastos Estatales (cuenta de gastos de operación y fondo rotatorio)	En proceso	Administrativo	1 años	5 años
Reportes Presupuestales	En proceso	Administrativo	1 años	5 años
Sistema Institucional de Archivos	En proceso	Administrativo	1 años	5 años

Programa Anual de Desarrollo Archivístico	En proceso	Administrativo	1 años	3 años
Solicitudes de Acceso a la información	En proceso	Administrativo y legal.	1 años	5 años
Solicitudes de Derecho Arco	En proceso	Administrativo y legal.	1 años	5 años
Seguimiento a comités de control interno de la administración pública Estatal.	En proceso	Administrativo	1 años	4 años
Auditoría Financiera	En proceso	Administrativo	1 años	5 años
Sesiones de junta de Gobierno	En proceso	Administrativo	1 años	5 años
Informes trimestrales de estados financiero	En proceso	Administrativo	1 años	5 años
Faltas administrativas	En proceso	Administrativo y legal.	3 años	10 años

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

Administrador	Usuario	Funciones
MTRO. MOISÉS JUÁREZ RODRÍGUEZ DIRECTOR GENERAL DE LA AGENCIA DE TECNOLOGÍAS E INNOVACIÓN DIGITAL	ING. LEONARDI HERRERA AGUILAR **JEFA DEL DEPARTAMENTO DE ATENCIÓN EN MESA**	• Recibir y registrar solicitudes de servicio. • Clasificar y priorizar Incidentes. • Brindar solución de Soporte de Primer Nivel de Atención. • Escalar incidencias a niveles superiores. • Dar seguimiento hasta la resolución. • Cerrar tickets y evaluar

		satisfacción del Usuario. • Elaboración y entrega de reportes semanales que reflejen las actividades realizadas, incidencias atendidas y avances obtenidos.
LIC. MARCELINO RAÚL GARCÍA MARTÍNEZ DIRECTOR JURÍDICO	LIC. ERASMO LUNA LÓPEZ **JEFE DEL DEPARTAMENTO DE NORMATIVIDAD EN TIC**	• Validar la elaboración de demandas, contestaciones y reconvenciones; interponer medios de impugnación e incidentes; así como ofrecer pruebas, formular alegatos y absolver posiciones, en los asuntos de la competencia de la Agencia. • Requerir a las Áreas Administrativas, la documentación e información que sea solicitada por las autoridades judiciales o administrativas; • Validar la elaboración de reglamentos, lineamientos, acuerdos, planes, circulares, convenios y contratos relacionados con asuntos de la competencia de la Agencia. • Revisar y presentar denuncias de hechos o querellas ante las autoridades correspondientes, sobre hechos constitutivos de delitos que afecten bienes o derechos de la Agencia, y presentar los desistimientos u otorgamiento del perdón que proceda
	MTRO. GUSTAVO	• Administrar los recursos

MTRO. EDGAR ROGELIO ESTRADA RUÍZ DIRECTOR ADMINISTATIVO	MORALES SALINAS **JEFE DEL DEPARTAMENTO DE RECURSOS FINANCIERON Y HUMANOS**	humanos y financieros, de conformidad con las normas y procedimientos establecidos por las instancias correspondientes. • Verificar el registro y control de los bienes muebles, inmuebles y equipos de la Agencia, asignados a las Áreas Administrativas conforme a las normas establecidas;
	ANADAIRA BUSTAMANTE SALINAS JEFA DEL DEPARTAMENTO DE RECURSOS MATERIALES Y SERVICIOS GENERALES	• Administrar los recursos, materiales y de servicios generales de conformidad con las normas y procedimientos establecidos por las instancias correspondientes. • Atender los requerimientos que le formulen las unidades administrativas del Órgano Garante en materia de recursos humanos y materiales; así como de planeación, administración presupuestal, financiera y contable.
MTRO. MANUEL ALEJANDRO GÓMEZ PÉREZ DIRECTOR DE DESARROLLO DE SISTEMAS	ING. CÉSAR SANTIAGO GUZMÁN **JEFE DEL DEPARTAMENTO DE DESARROLLO DE SISTEMAS WEB**	• Instruir la implementación de Soluciones Tecnológicas en materia de Software que optimicen los procesos, trámites y servicios de las Entidades y Entidades de la APE; • Supervisar los proyectos relacionados con la adquisición e implementación de Soluciones Tecnológicas en materia de Software de las Entidades y Entidades de la APE;

3. Análisis de Riesgo.

Para dar cumplimiento al artículo 27 fracción IV de la Ley General de Datos Personales en Posesión de Sujetos Obligados, el responsable deberá realizar un análisis de riesgos de los Datos Personales considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

Unidad Administrativa	Núm. de Titulares de Datos Personales
Indicar el área que recaba Datos Personales	Indicar el número de Titulares (personas) de las cuales recaban Datos Personales.
Departamento de Atención en Mesa (Mesa de ayuda)	**2033 titulares**
Dirección Jurídica	**251 titulares**
Dirección Administrativa	**298 titulares**
Dirección de Desarrollo en Sistemas	**2482 titulares**
Total de Titulares de Datos Personales	**5064 titulares**

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 datos	Nivel de Riesgo Inherente
Identificación	Bajo
Contacto	Bajo
Académicos	Bajo
Patrimoniales	Inherente medio
Laboral	Inherente medio
Familiares	Inherente medio
Bancarios	Inherente reforzado
Salud	Inherente alto
Biométricos	Inherente alto

4. Análisis de Brecha.

4.1. Medidas de seguridad existentes.

ÁREA	MEDIDAS DE SEGURIDAD EXISTENTES
Departamento de Atención en Mesa (Mesa de ayuda)	Física: Medidas de seguridad de acceso a las instalaciones de esta Agencia, puerta para acceder a esa área, archiveros y cajones con llave para el resguardo de documentos, avisos de privacidad Técnica: Computadora con usuario y contraseña, acceso a sistemas con usuario y contraseña (PNT, correos electrónicos, Sistema de ética e integridad y sistema de registro de entidades paraestatales).
Dirección Administrativa	Física: Medidas de seguridad de acceso a las instalaciones de esta Agencia, puerta para acceder a esa área, archiveros y cajones con llave para el resguardo de documentos, avisos de privacidad Técnica: Computadora con usuario y contraseña, acceso a sistemas con usuario y contraseña (PNT, correos electrónicos, Sistema de ética e integridad y sistema de registro de entidades paraestatales).
Dirección Jurídica	Física: Medidas de seguridad de acceso a las instalaciones de esta Agencia, archiveros y cajones con llave para el resguardo de documentos, avisos de privacidad Técnica: Computadora con usuario y contraseña, acceso a sistemas con usuario y contraseña (PNT, correos electrónicos, Sistema de ética e integridad y sistema de registro de entidades paraestatales).
Dirección de Desarrollo de Sistemas	Física: Medidas de seguridad de acceso a las instalaciones de esta Agencia, archiveros y cajones con llave para el resguardo de documentos, avisos de privacidad

	Técnica: Computadora con usuario y contraseña, acceso a sistemas con usuario y contraseña (PNT, correos electrónicos, Sistema de ética e integridad y sistema de registro de entidades paraestatales).

4.2. Medidas de Seguridad faltantes.

Para una mejor implementación e identificación de las medidas de seguridad, se debe considerar lo establecido en los artículos 26 y 27 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados donde establecen principios para que se utilicen como base para la selección de medidas de seguridad, y de este modo se encuentren alineadas a la protección de datos personales.

Por lo anterior, las medidas de seguridad que la Agencia de Tecnologías e Innovación Digital, requiere implementar serán utilizadas para reforzar la seguridad de los datos personales.

Medidas de seguridad a implementar	Tipo de medida de seguridad
Capacitaciones	Administrativa
Seguridad en el almacenamiento de datos físicos: Aumentar el número de archiveros con llave de seguridad en las oficinas en que se resguardan documentos físicos que contengan datos personales.	Física
Mantenimiento a equipos tecnológicos: llevar a cabo de forma periódica el mantenimiento y actualización a los equipos de cómputo y tecnológicos que se utilizan para acceder y resguardar datos personales.	Técnica
Mantenimiento a software y sistemas: Solicitar mantenimiento y actualización a los sistemas que guardan datos personales.	Técnica
Control de contraseñas y accesos de equipos: Realizar periódicamente cambio de contraseñas para acceder a las computadoras y equipos tecnológicos que utilizan y resguardan datos.	Técnica
Control de contraseñas y accesos de	Administrativa

usuarios de sistemas; realizar periódicamente eliminación de usuarios que han dejado de hacer uso de los sistemas, así como el cambio de contraseñas de seguridad de los usuarios activos para acceder a los sistemas que utilizan y guardan datos personales.	

5. Plan de Trabajo.

Posterior a la revisión de acciones existentes y a implementar, se propone el siguiente plan de trabajo con el objetivo de fortalecer las capacidades del personal de la Agencia en materia de implementación y cumplimiento de medidas.

ACCIONES A IMPLEMENTAR	Indicar si la acción se realizará de manera mensual, bimestral o trimestral		
	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	
Aumentar el número de archiveros con llave de seguridad en las oficinas en que se resguardan documentos físicos que contengan datos personales.			X
Mantenimiento a equipos de cómputo		X	
Mantenimiento a software y sistemas			X
Cambios periódicos de contraseñas			X
Control de contraseñas y accesos de usuarios de sistemas.			X

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

Las medidas de seguridad propuestas a implementar en cada una de las áreas de la Agencia de Tecnologías e Innovación Digital se evaluarán de manera Bimestral y Trimestral, tanto las medidas de seguridad administrativas como las técnicas para determinar su eficacia vulnerabilidad.

Monitoreo de las medidas de seguridad	Indicar si la acción se realizará de manera mensual, bimestral o trimestral		
	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**
Aumentar el número de archiveros con llave de seguridad en las oficinas en que se resguardan documentos físicos que contengan datos personales.			**X**
Mantenimiento a equipos de cómputo			**X**
Mantenimiento a software y sistemas			**X**
Cambios periódicos de contraseñas			**X**
Control de contraseña y accesos de usuarios de sistemas			**X**

7. Programa general de capacitación.

Con la finalidad de garantizar que las y los servidores públicos de la Agencia de Tecnologías e Innovación Digital, cuenten con conocimientos que permitan contribuir a un adecuado tratamiento de los expedientes que contienen datos personales se ha programado realizar capacitaciones en los siguientes temas:

Temas de capacitación	Indicar si la acción se realizará de manera mensual, bimestral o trimestral		
	Mensual	Bimestral	Trimestral
Principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados			x
Responsabilidades administrativas de las personas servidoras públicas			x

INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DE LA AGENCIA DE TECNOLOGÍAS E INNOVACIÓN DIGITAL

MTRA. FELICITAS MARTÍNEZ GÓMEZ.

PRESIDENTA.

LIC. ERASMO LUNA LÓPEZ

SECRETARIO TÉCNICO.

LIC. VÍCTOR ÁNGEL ÁVILA SANTIAGO

VOCAL.

LIC. MARCELINO RAÚL GARCÍA MARTÍNEZ.

INVITADO PERMANENTE Y TITULAR DE LA UNIDAD DE TRANSPARENCIA

MTRO. GUSTAVO MORALES SALINAS

INVITADO ESPECIAL Y OFICIAL DE DATOS PERSONALES.

Mediante acuerdo **ACUERDO/ATID/CT/01EXT/01/2026,** de fecha doce junio de 2026, aprobado por el Comité de Transparencia de la Agencia de Tecnologías e Innovación Digital, de conformidad con los artículos 29, 30, 78 fracción I y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se aprobó el presente Documento de Seguridad para el Tratamiento de los Datos Personales.