Archivo General
del Estado de Jalisco

Documento de Seguridad del Archivo General del Estado de Jalisco, AGEJ.

2025

JALISCO
GOBIERNO DEL ESTADO

INDICE.

1. INTRODUCCIÓN:

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios se establecen las bases, principios, procedimientos y tratamientos que permiten garantizar la protección de datos personales de los ciudadanos en posesión del organismo como sujeto obligado.

Teniendo como base dicha normatividad y de conformidad con lo que establece en los artículos 3 fracción XIV y los artículos del 30 al 44, así como la Guía para Elaborar un Documento de Seguridad emitida por el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco; se crea el presente documento de seguridad.

Desde la emisión de la Ley en referencia, el día 1 de abril del año 2025, el AGEJ a través de la Unidad de Transparencia, en conjunto con los enlaces que esta tiene en cada área generadora de información, han realizado acciones y actividades que tuvieron como finalidad establecer los cimientos para la creación de este documento.

De entre las mismas, destaca la elaboración de un listado de datos personales que nos permitió identificar información básica sobre el tratamiento al que son sometidos por cada área del AGEJ y hacer el primer acercamiento con las áreas sobre la importancia del resguardo de los datos personales. Este documento permitió identificar los trámites que realiza el AGEJ y en consecuencia trajo la creación del sistema de tratamiento de datos personales sobre los mismos.

2. Medidas de Seguridad Implementadas y Procedimientos de Respaldo y Recuperación de Datos Personales:

MEDIDA	DESCRIPCIÓN
Control de servidores públicos que recaban los datos personales	Debe realizarse un listado de los servidores públicos que recaban datos personales y/o que tienen contacto con el titular de los datos personales por sus funciones. Actualización del listado: cada 12 meses.
	Forzosa asistencia a por lo menos a una capacitación en materia de datos personales
	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Obtención de datos personales	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos deberá pedir al ciudadano acredite su identidad.

Aviso de Privacidad	El servidor público que reciba los datos personales deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.
	Si el trámite del cual se recabarán datos personales cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del AGEJ, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado.
	Si el trámite del cual se recabarán datos personales fue obtenido mediante una plataforma electrónica oficial, esta deberá contener la mención, así como dar a conocer el aviso de privacidad del AGEJ, ya sea simplificado o la liga de internet que remita al ciudadano al Aviso Integral.
Espacio físico	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área.
	El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de estos o vulneraciones.
	Las llaves de las puertas de cada dependencia deberán ser guardadas únicamente por personal de seguridad y/o los servidores públicos del área, autorizados para poseer las llaves.
	Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados.
	Al concluir la jornada laboral, se deberán guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Resguardo provisional, durante el desahogo del trámite	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté

	fuera del alcance de los ciudadanos, ya sea en una caja, archivero o mueble.
Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes, estos deberán archivarse en un lugar adecuado con las siguientes características: · No estar al alcance de los ciudadanos o servidores públicos ajenos al área. · Deberá ser un área específica para guardar los expedientes. · Este archivo debe estar bajo llave. · La llave de este solo puede estar en manos de un servidor autorizado para esto.
Acceso al archivo	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener lo siguiente: · Registro para anotar el nombre y puesto del servidor público autorizado. · Fecha, hora de entrada y hora de salida del archivo. · Registrar el expediente que se consultó. · Registrar el expediente que se extrae del archivo y la fecha en la que se regresa el expediente. · Firma de conformidad del servidor público que entró. · Firma de consentimiento del servidor público autorizado para llevar el control de este archivo.
Control de archivos electrónicos	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada.
	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Inventarios Documentales sobre archivos entregados a la Coordinación de Archivos	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos que se mandan a la Coordinación de Archivo para su resguardo en el Archivo de Concentración del AGEJ.

Transferencia de datos personales	En caso de ser necesario, derivado de las funciones de los servidores públicos o por requisito de algún trámite, se deba realizar una transferencia de datos personales, así como informar al sujeto que reciba los datos del aviso de privacidad, para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan dichos datos deberán entregarse siempre en versión pública.
Archivo finalizado	Al momento de finalizar el trámite, todos los expedientes deberán desecharse y enviarse al archivo de concentración, conforme a la normatividad correspondiente.

2.1. Controles y Mecanismos de Seguridad para las Transferencias:

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, exceptuando las realizadas entre responsables en cumplimiento de una disposición legal o en el ejercicio de sus atribuciones, así mismo en el ámbito internacional cuando se encuentren previstas en una ley o tratado internacional suscrito y ratificado por México, o sea solicitada por una autoridad u organismo internacional competente.

Transferencias mediante el traslado de soportes físicos:

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo que son implementados para proteger el hardware y medios de almacenamiento de datos.

Transferencias mediante el traslado físico de soportes electrónicos:

En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles, sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello, es cuando una dependencia entrega a otra por mensajería

oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

Al realizar transferencias físicas de soportes electrónicos, se deberá considerar los dispuesto en los ordenamientos aplicables, como lo son: Los oficios de comisión para el personal autorizado y asegurar que la entrega sea a los titulares de la información o a personal autorizado para recibirla, los medios para garantizar la confidencialidad de la información, utilizar las leyendas de clasificación, registro en bitácoras de transferencia, cifrar la información, utilizar contraseñas, etc.

Transferencias mediante el traslado sobre redes electrónicas:

En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.
- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales tratándose de procedimientos de derecho ARCO.

Transferencias a terceros:

- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado, así como adoptar las medidas de seguridad previstas en este documento.
- En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

2.2. Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales:

BITÁCORAS DE ACCESO	1. Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede. • Identificación del Expediente. • Fojas del Expediente. • Propósito del Acceso. • Fecha de Acceso. • Hora de Acceso. • Fecha de Devolución. • Hora de Devolución. 2. Las bitácoras se encuentran en soporte físico o electrónico. 3. Son resguardadas por los coordinadores de cada área en el lugar que para tal efecto designen, el cual, debe estar resguardado bajo llave.
VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES	La bitácora de vulneraciones contendrá la siguiente información: • Nombre de quien reporta el incidente • Cargo • La fecha en la que ocurrió; • El motivo de la vulneración de seguridad; y • Las acciones correctivas implementadas de forma inmediata y definitiva.

2.3. Controles para la Identificación y Autenticación de Usuarios:

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público.

En el ambiente electrónico todas las computadoras precisan de un nombre de usuario y contraseña para ingresar. La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de tecnologías de la información. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario, también permite la utilización personalizada de acceso a la información y generación de esta.

Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado.

El estándar para la creación de las cuentas es:

Usuario: Generalmente es el correo electrónico institucional

Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad.

Los empleados del organismo deben portar su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre.
- Cargo.
- Número de empleado.
- Vigencia.

Al reverso:

- Sitio oficial de la Institución.
- Firma del Titular de la Institución.
- Número de Seguridad Social.
- Firma del empleado.

Toda persona que ingresa a las instalaciones también se debe identificar y registrar en la bitácora de seguridad correspondiente. A los ciudadanos se les solicitará identificación oficial con fotografía únicamente cuando sea necesario que acrediten su identidad ante el AGEJ como sujeto obligado.

3. Técnicas de Seguridad para la Supresión y Borrado de Datos Personales:

Todos los datos personales en posesión del sujeto obligado sin importar el soporte en el que se encuentren deberán ser tratados para la supresión y borrado conforme a lo establecido en la Ley General de Archivos y en la Ley de Archivos del Estado de Jalisco y sus Municipios.

De conformidad con el artículo 3 fracción V de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, el bloqueo se dará únicamente después del cumplimiento de la finalidad con la que fueron recabados los datos personales, hasta que cumpla el plazo de prescripción legal o contractual correspondiente, concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente que corresponda y al mismo tiempo se está garantizando la supresión de los datos personales.

Bases para supresión y borrado seguro de archivos:

I. Las bajas documentales se realizan mediante la aprobación del Comité de Archivo del AGEJ.
II. Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador y son vigilados por personal del AGEJ hasta su destino final, en donde son triturados.

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobrescritura en la totalidad del área de almacenamiento de la información.

3.1. Desmagnetización:

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como, por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

3.2. Destrucción física:

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: desintegración, pulverización, fusión e incineración, estos son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos.

Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado. Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

3.3 Sobre-escritura

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. Esta técnica se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

4 Análisis de Riesgos

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación con la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante los riesgos identificados anteriormente, es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones, tales como:

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del AGEJ.	Adquirir información o datos personales.	- Acceso no autorizado. - Divulgación de datos personales. - Robo de información. - Modificaciones no autorizadas.
Acceso a criminales o traficantes de datos a los sistemas o plataformas oficiales de AGEJ	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	- Extorsiones. - Ataques a personas. - Robo de información. - Vulneración a la seguridad física y mental de los ciudadanos.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	- Obtener información para beneficio personal. - Curiosidad. - Error involuntario.	- Ataque a otros servidores públicos. Robo de información. - Pérdida de datos personales.

	- Por fines económicos.	- Uso indebido de datos personales. - Uso ilícito de datos personales. - Extorsión. - Modificaciones no autorizadas. - Robo de información.
Daño físico.	- Agua. - Fuego. - Accidentes. - Corrosión.	- Daño o pérdida de los datos personales.
Eventos naturales.	- Desastres climatológicos. - Fenómenos meteorológicos. - Sismos. - Cualquier eventualidad por causa natural.	- Daño o pérdida de los datos personales.
Fallas técnicas.	- Pérdida de electricidad. - Falla o pérdida de internet. - Falla en sistemas, correos electrónicos o plataformas oficiales.	- Daño o pérdida de los datos personales. - Divulgación y transferencia de datos personales. - Modificaciones no autorizadas.
Decadencias técnicas.	- Mantenimiento insuficiente. - Falla en equipos. - Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	- Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	- Falta de contraseñas altamente efectivas.	- Pérdida, destrucción y daño. - Divulgación y transferencia de datos personales.

	- Falta de mecanismos para identificar o autentificación de usuarios. - Falta de actualización de antivirus.	- Modificaciones no autorizadas. - Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	- Pérdida, destrucción y daño. - Divulgación y transferencia de datos personales. - Modificaciones no autorizadas. - Robo de información.
Espacio donde se archiven.	- Carencia de espacio. - Espacio con poca seguridad. - Espacio no adecuado. - Falta de llaves o medidas de seguridad para accesos.	- Daño o pérdida de los datos personales. - Divulgación y transferencia de datos personales. - Modificaciones no autorizadas. Robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	La carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	- Daño y/o pérdida de los datos personales. - Modificaciones no autorizadas.

5. Gestión de Vulneraciones:

En caso de ocurrir alguna vulneración, deberá registrarse en la bitácora de contingencias, misma que deberá seguirse bajo el siguiente formato y ejemplo:

FECHA	MOTIVO DE LA VULNERACIÓN	LAS ACCIONES CORRECTIVAS IMPLEMENTADAS DE FORMA INMEDIATA Y DEFINITIVA
19/03/2025*	Sismo*	Generación de nuevo expediente electrónico*

*Ejemplo

5.1. Plan de Respuesta:

Después del registro, se deberá informar de forma inmediata al titular y al organismo las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

I. La naturaleza del incidente.
II. Los datos personales comprometidos.
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
IV. Las acciones correctivas realizadas de forma inmediata.
V. Los medios donde se puede obtener más información al respecto.

Al ocurrir una vulneración de seguridad, el servidor público titular del área responsable y/o el responsable del sistema, deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita. A su vez, en caso de detectar que la falla fue ocasionada por el incumplimiento de un servidor público a su cargo, deberá levantar acta circunstanciada de hechos correspondiente y seguir el procedimiento administrativo correspondiente ante el Órgano Interno de Control del AGEJ.

6. Los mecanismos de monitoreo y revisión de las medidas de seguridad:

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas para el IDEFT.

MECANISMO DE MONITOREO	OBJETIVO

Visitar a 2 áreas generadoras de información cada 12 meses, las áreas serán elegidas de forma aleatoria.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear y revisar avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

7. Análisis de Brecha:

Una vez identificados los posibles riesgos a los que el AGEJ como Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con cada enlace que tiene la Unidad de Transparencia con diferentes áreas generadoras de información.

Las áreas administrativas informaron sobre las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales es un servidor público del área asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales se encuentra dentro de las instalaciones.
- Cuando los datos personales son recabados de forma digital, se recaban por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir, si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio del cual se obtuvieron los datos personales ya sea físico o electrónico.
- Una vez recabados los datos personales y realizada la carpeta o expediente (electrónico, físico, en plataformas, etc.) se guarda en archiveros o es puesto en resguardo electrónico, tienen acceso a esta área solo los servidores públicos adscritos a esta.

● Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.

● Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.

● Durante el desahogo del trámite del cual se obtuvieron los datos personales solo los servidores públicos del área tienen acceso a estos.

● Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

●Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del AGEJ.

El riesgo latente es la falta de conocimiento o ausencia compromiso para la aplicación de estas medidas existentes.

El riesgo identificado en líneas anteriores se puede minimizar por medio del establecimiento obligatorio de las medidas de seguridad que deben ser actualizadas y mejoradas de manera periódica.

8. Plan de Trabajo:

La existencia del documento de seguridad busca enmarcar los deberes del Archivo General del Estado de Jalisco, para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el Organismo realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará con base a las atribuciones establecidas en la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.

2. Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

3. Se buscará la participación de las autoridades competentes en materia de transparencia para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.

2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para el AGEJ.

3. Actualizar el presente plan de trabajo.

4. Se emitirá un programa anual de capacitaciones y además se promoverá que el personal del AGEJ se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

9. Programa General de Capacitación:

Se manejarán las capacitaciones de conformidad al Plan Anual de Trabajo de la Unidad de Transparencia del AGEJ y con las necesidades de este sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado.

Las fechas exactas se les notificarán a los Enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.

10. Plan de Contingencia:

Ante la pérdida total o parcial de datos personales en posesión del AGEJ como sujeto obligado debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que nos encontramos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior, toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual, existan riesgos inminentes que día a día evolucionan.

Con la aplicación de las medidas de seguridad establecidas en este documento, se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

11. Catálogo de Sistemas de Tratamiento de Datos Personales:

SISTEMA DE TRATAMIENTO PARA LA CONTRATACIÓN DE PERSONAL			
Administrador:	**Eréndira Hernández Vega**	**Bases de datos**	**-Expediente de personal. -Sistema de pagos. - Sistema de Pensiones del Estado de Jalisco.**
Cargo:	**Jefatura de Recursos Humanos del AGEJ**		
Área:	**Dirección de Administración**		
Funciones y obligaciones:	**Planificar, dirigir y coordinar las actividades del personal y las relaciones laborales del AGEJ.**		
PERSONAL AUTORIZADO PARA TRATAMIENTO			
Directora Administrativa	**Georgina Marcela Arellano Anguiano**	**Bases de datos**	**-Expediente de personal. -Sistema de pagos. - Sistema de Pensiones del Estado de Jalisco.**
Funciones y obligaciones:	**Directora de Administración**		
Jefa de Recursos Humanos	**Eréndira Hernández Vega**	**Bases de datos**	**-Expediente de personal. -Sistema de pagos. - Sistema de Pensiones del Estado de Jalisco.**
Funciones y obligaciones:	**Jefatura de Recursos Humanos del AGEJ**		
TIPO DE DATOS PERSONALES PERTENECIENTES AL SISTEMA DE TRATAMIENTO			

Inventario:	**Nombre, edad, sexo, fecha de nacimiento, lugar de nacimiento, domicilio particular, correo electrónico personal, teléfonos particulares, credencial electoral, documentos oficiales que acrediten su personalidad, número de identificación diversa, estado civil, firma particular, fotografía, CURP, RFC, número de cuenta bancaria, patrimonio, parentesco, nombre de familiares, grado académico, reconocimiento facial, huellas digitales, estado de salud.**
Bases de datos:	**- Expediente de personal. - Sistema de pagos. - Sistema de Pensiones del Estado de Jalisco.**
No. De titulares:	**- 5k Datos entre 501 hasta 2,000 personas.**
Controles de seguridad para las bases de datos:	**- Control de servidores públicos que recaban los datos personales. - Obtención de datos personales. - Aviso de Privacidad. - Espacio físico. - Resguardo provisional, durante el desahogo del trámite. - Archivo, al finalizar el desahogo del trámite. - Acceso al archivo.**
ESTRUCTURA Y DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO	
Tipo de soporte:	**- Físico. - Electrónico.**
Características del lugar de resguardo:	**- Archiveros dentro de oficina bajo llave.**
Programas en que se utilizan los Datos Personales:	**- Windows 10. - Nomipaq - SAACG.net - SAT**

	- **SEPIFAPE** -
RESGUARDO DE LOS EN QUE SE ENCUENTRAN LOS DATOS PERSONALES	
Físicos:	- **Computadoras protegidas por contraseña de acceso y archiveros bajo el resguardo de Georgina Marcela Arellano Anguiano y Eréndira Hernández Vega.**
Electrónicos:	
LAS BITÁCORAS DE ACCESO Y OPERACIÓN COTIDIANA	
Bitácoras físicas:	- **Jefatura de Recursos Humanos del AGEJ.**
Clave de la bitácora:	- **Bitácora de Acceso a Datos Personales de la Jefatura de Recursos Humanos del Archivo General del Estado.** - **Soporte físico.** - **Eréndira Hernández Vega** - **Jefatura de Recursos Humanos del Archivo General del Estado.**
Bitácoras electrónicas:	- **Jefatura de Recursos Humanos del AGEJ.**
Clave de la bitácora:	- **Bitácora de Acceso a Datos Personales de la Jefatura de Recursos Humanos del Archivo General del Estado.** - **Soporte electrónico.** - **Eréndira Hernández Vega** - **Jefatura de Recursos Humanos del Archivo General del Estado.** - **Computadora protegida por contraseña de acceso dentro de oficina bajo llave.**

LAS BITÁCORAS DE VULNERACIONES DE SEGURIDAD	
Soporte	**Responsable**
Electrónico	**Eréndira Hernández Vega**

SISTEMA DE TRATAMIENTO PARA EL INGRESO DEL ALUMNADO			
Administrador:	**Alberto Ramirez Martinez**	**Bases de datos**	**-Expediente y bitácoras de capacitaciones a sujetos obligados**
Cargo:	**Jefatura de Capacitación y cultura archivística del AGEJ**		
Área:	**Dirección DE ARCHIVO**		
Funciones y obligaciones:	**Desarrollar, complementar, perfeccionar o actualizar los conocimientos y habilidades necesarios para el eficiente desempeño de los servidores públicos en materia de archivos.**		
PERSONAL AUTORIZADO PARA TRATAMIENTO			
Director de Archivos.	**Saúl Gabriel Vite Téllez**	**Bases de datos**	**--Expediente y bitácoras de capacitaciones a sujetos obligados**
Funciones y obligaciones:	**Desarrollar, complementar, perfeccionar o actualizar los conocimientos y habilidades necesarios para el eficiente desempeño de los servidores públicos en materia de archivos.**		
Jefe de Capacitación y cultura archivística.	**Alberto Ramirez Martinez**	**Bases de datos**	**--Expediente y bitácoras de capacitaciones a sujetos obligados**

Funciones y obligaciones:	**Desarrollar, complementar, perfeccionar o actualizar los conocimientos y habilidades necesarios para el eficiente desempeño de los servidores públicos en materia de archivos.**
TIPO DE DATOS PERSONALES PERTENECIENTES AL SISTEMA DE TRATAMIENTO	
Inventario:	**Solicitud de inscripción:** Nombre, edad, sexo, lugar de nacimiento, RFC, datos de un familiar, domicilio personal, correo electrónico, discapacidad, pertenencia a alguna comunidad indígena y grado académico. **Identificación Oficial o acta de nacimiento:** fecha de nacimiento, lugar de nacimiento, nombres de terceros, domicilio particular, edad, sexo, curp, clave de elector, folio de identificación, firma particular y fotografía. **Comprobante de domicilio:** Domicilio personal.
Bases de datos:	**- Expedientes de capacitados**
No. De titulares:	**- Un aproximado de 686 capacitados al mes de julio del año 2025.**
Controles de seguridad para las bases de datos:	- **Control de servidores públicos que recaban los datos personales.** - **Obtención de datos personales.** - **Aviso de Privacidad.** - **Espacio físico.** - **Resguardo provisional, durante el desahogo del trámite.** - **Archivo, al finalizar el desahogo del trámite.** - **Acceso al archivo.**
ESTRUCTURA Y DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO	
Tipo de soporte:	- **Físico.** - **Electrónico.**

Características del lugar de resguardo:	- **Archiveros dentro de oficina bajo llave.**
Programas en que se utilizan los Datos Personales:	- **Windows 10.**
RESGUARDO DE LOS EN QUE SE ENCUENTRAN LOS DATOS PERSONALES	
Físicos:	**- Expedientes resguardados en oficinas en archiveros protegidos con llave.**
Electrónicos:	**- Computadoras protegidas por contraseña de acceso y archiveros bajo el resguardo de Jefe de Capacitación y cultura archivística.**