Documento de Seguridad para la Protección de Datos Personales en Posesión de la Auditoría Superior del Estado de Jalisco.

El presente documento tiene como objeto describir y dar cuenta de manera general las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Auditoría Superior del Estado de Jalisco para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, con base en los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

La Auditoría Superior del Estado de Jalisco es el órgano técnico profesional y especializado de revisión y examen del Congreso del Estado de Jalisco, dotado de autonomía técnica y gestión para decidir sobre su organización interna, funcionamiento y resoluciones, en los términos que dispone la Ley de Fiscalización Superior y Rendición de Cuentas del Estado de Jalisco y sus Municipios, y considerado sujeto obligado, según lo señalado por el artículo 24 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y el artículo 3.1 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

El objetivo que tiene esta Auditoría Superior es el de fiscalizar las cuentas públicas, y auditar los ingresos, los egresos, el manejo, la custodia y la aplicación de fondos, recursos, deuda pública, y el destino y ejercicio de los recursos obtenidos mediante empréstitos u obligaciones de los órganos del poder público, los ayuntamientos, los organismos públicos autónomos, los organismos públicos descentralizados, la Universidad de Guadalajara, los fideicomisos públicos y las empresas de participación pública estatal o municipal mayoritaria.

Glosario

Auditoría Superior	La Auditoría Superior del Estado de Jalisco
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Disociación	El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.
DMZ	En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de *demilitarized zone*) o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (*hosts*) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (*hosts*) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (*host*) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.
DNS	Un Servidor DNS en informática responde a las siglas *Domain Name System*. Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada.
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.
Encargado	Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales	Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto	Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
LAN	Una red de área local o LAN (por las siglas en inglés de *Local Area Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley General de Transparencia	Ley General de Transparencia y Acceso a la Información Pública.
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar los protección, confidencialidad, disponibilidad e integridad de 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, formación 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.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

N/A	No aplica.
Responsable	Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
SGSI	El Sistema de Gestión de Seguridad de la Información (SGSI), es un sistema que identifica los diversos activos (personas, hardware, software, documentos, etc.), para llevar a cabo un análisis de los riesgos a los que pueden estar expuestos y realizar acciones que permitan minimizar el impacto en caso de presentarse. Todo esto para garantizar la confidencialidad, la integridad y la disponibilidad de dichos activos.
Supresión	La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
Titular	Persona física a quien pertenecen los datos personales.
Transferencia	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.
Tratamiento	De manera enunciativa más son limitativa 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.

Inventario de datos personales y de los sistemas de tratamiento.

La Ley General y Ley definen dos tipos de datos personales, primero los datos personales, que es cualquier información concerniente a una persona física identificada o identificable, para lo que se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. El otro tipo, son los datos personales sensibles, que son aquellos que se refieran a las esfera más íntima, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, para enunciar algunos se consideran sensibles los datos que revelan aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas o morales, así como las opiniones políticas o preferencia sexual, etc.

La Auditoría Superior, como órgano técnico y especializado de revisión y examen, tiene acceso a diferentes inventarios de datos personales, que los distribuye en los respectivos sistemas de tratamientos que pueden ser consultados en el apartado del catálogo de estos. Se señala de forma generaliza el tipo de datos personales con los que tiene trato para su conocimiento, con base en lo que establece en las atribuciones de este sujeto obligado descritas en el artículo 13 de la Ley de Fiscalización Superior y Rendición de Cuentas del Estado de Jalisco y sus Municipios, por lo que tiene acceso a los siguientes datos personales:

Datos personales de servidores públicos estatales y municipales	Direcciones personales; edades; correos personales; números de teléfono celular; claves del Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP); número de seguridad social, copias de identificación oficial, actas de nacimiento; firmas; comprobantes de domicilio; nacionalidad; fecha de nacimiento;
Datos personales de beneficiarios y beneficiarias de programas públicos	Nombres; Direcciones particulares; clave de elector; clave del Registro Federal de Contribuyentes (RFC); Clave única del Registro de Población (CURP);
Datos personales de procedimientos administrativos	Nombres de personas físicas; clave del Registro Federal de Contribuyentes (RFC); Dirección fiscal de personas físicas; teléfonos fijos o celulares de personas físicas; correos electrónicos de personas físicas; Cuentas bancarias de personas físicas;
Datos personales sensibles de servidores públicos	Género; grupo sanguíneo y factor RH; alergias; discapacidades; enfermedades; certificados médicos;

Las funciones y obligaciones de las personas que traten datos personales.

Dentro de cada uno de los sistemas de tratamiento incluidos en este documento se especifican las funciones y obligaciones para aquellos servidores públicos que se encuentran en contacto, resguardo y la transferencia de datos personales. En términos generales, dentro de las obligaciones es el de hacer responsable a cualquier servidor público que tiene bajo su resguardo información que contiene datos personales, archivos físicos y electrónicos con fundamento y guardar congruencia con las atribuciones existentes en el Reglamento Interno de la Auditoría Superior del Estado de Jalisco.

Los auditores especiales, directores generales y directores de la Auditoría Superior deben asegurarse de que el personal a su cargo y con acceso físico o automatizado a los repositorios de datos personales conozcan: a. Las normas de seguridad que deben observarse para su tratamiento; b. sus atribuciones respecto a los sistemas de tratamiento; c. las responsabilidades que tienen, junto con la firma de la carta de responsiva y confidencialidad; d. las consecuencias en caso de incumplimiento de las atribuciones, resguardo o la vulneración de los datos personales.

Dentro de los Lineamientos Generales de Protección de Datos Personales para el Sector Gobierno, si bien es cierto habla de la obligación que tiene el Responsable de los tratamientos de los datos personales, entendiendo como responsable al titular del sujeto obligado, sin embargo durante el manejo, tratamiento, transferencia , divulgación, uso de los mismos intervienen en este tránsito de información más personas, de esta manera encontramos en dichos lineamiento en el artículo 56 específicamente en la fracción II y III el establecimiento de los roles, responsabilidades y sanciones por incumplimiento en el tratamiento de los datos personales, por parte de los involucrados internos o externos, el mismo remite al artículo 33 I ,II de la Ley General y 32 I y II de la Ley.

Análisis de riesgos.

Se eliminaron dos párrafos con cinco y cuatro renglones , respectivamente por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Se eliminaron dos párrafos con cinco renglones y tres, respectivamente por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de brecha.

Se eliminaron dos párrafos con seis y cinco renglones, respectivamente por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Plan de trabajo.

De acuerdo al artículo 33 VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como a los artículos 33, y 34 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, es necesaria la implementación de un Plan de Trabajo ya que se encuentra descrita como una de las obligaciones que al menos debe contener el documento de seguridad.

Actividades	Temporalidad	Áreas involucradas	Actualización
Creación de políticas internas para el tratamiento de datos personales	Anual	Delimitación del personal que maneja datos personales en todas las direcciones.	En acontecimientos que se susciten y los lineamientos que se publiquen

Revisión de los inventarios de datos personales	Anual	Todas las direcciones	Mensual
Actualización, realización y monitoreo de la bitácora del manejo de datos personales.	Anual	Comunicación directa con el responsable de la realización de la misma, en cada dirección.	Mensual
Establecer comunicación directa con la Unidad de Transparencia en relación a cuestionamientos relativos a la protección de datos personales.	Siempre que sea necesaria	Director de área, Enlace de transparencia, o cualquier persona que maneje datos personales	Siempre que sea necesaria
Seguimiento al plan de capacitación en relación a la protección de datos personales	Según la temporalidad de las sesiones establecidas	Personal que maneje datos personales	Mensual
Revisión periódica de las medidas de seguridad señaladas en el documento de seguridad.	Mensual	Personal que maneje datos personales	Mensual
Formular el análisis y matriz de riesgos	Anual	Personal que maneje datos personales	Mensual

Mecanismos de monitoreo y revisión de las medidas de seguridad.

Las medidas de seguridad adoptadas por la Auditoría Superior, con base en la Ley General y la Ley en la materia, consideran:

a) El riesgo inherente a los datos personales tratados;
b) La sensibilidad de los datos personales tratados;
c) El desarrollo tecnológico;
d) Las posibles consecuencias de una vulneración para los titulares;
e) Las transferencias de datos personales que se realicen;
f) El número de titulares;
g) Las vulneraciones previas ocurridas en los sistemas de tratamiento; y

h) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Por esa razón se generaron acciones que establecen el mantenimiento de las medidas de seguridad en las cuales de manera general se destaca que el objeto de las mismas es la protección de los datos personales, y para ello al menos se consolidarán las siguientes acciones interrelacionadas:

1. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
2. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
3. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
4. Realizar un análisis de riesgo 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 responsable, entre otros;
5. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
6. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
7. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y
8. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Acciones que en buena medida se encuentran desarrolladas en este documento de seguridad, donde se enuncian dichas obligaciones, análisis y seguimiento de las mismas, a fin de poderlas incluir para la siguiente actualización en las políticas que ya existen dentro del Sistema de Gestión de Seguridad de la Información. En el análisis que se hagan de las políticas ya existentes se deberán utilizar los siguientes elementos:

- Que existan controles en donde se garantice la validación, confidencialidad, integridad y disponibilidad de los datos personales en posesión de esta Auditoría Superior;
- Que se cuente con las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;
- Mantenerse atentos para implementar las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;
- Contar con un proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;
- Tener la seguridad adecuada para que los controles garanticen que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento, y

- Implementar las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas.

La Auditoría Superior deberá analizar todas las causales de ocurrencia de una vulneración a fin de implementar dentro del plan de trabajo las acciones preventivas y correctivas que se ajusten con las medidas de seguridad correspondiente para dar el tratamiento de los datos personales adecuados, a fin de evitar que el riesgo de vulnerabilidad persista.

También se establecerán controles y mecanismos que tengan el objetivo para que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo, a través de cartas de responsabilidad que serán firmadas por cada uno de los servidores públicos o personas externas a esta Auditoría Superior; sin menoscabo de lo establecido en las disposiciones aplicables en materia de acceso a la información pública.

Las medidas de seguridad son conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales, y las cuales se pueden definir y agrupar de la siguiente manera:

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, formación 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. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En relación al monitoreo de la seguridad es de observarse lo dispuesto en el artículo 63 los Lineamientos Generales de Protección de Datos Personales para el Sector público, el cual refiere que se deberá elaborar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Las acciones a monitorear son los siguientes:

- Los nuevos activos que se incluyen en la gestión de riesgos;
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras;
- Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a este punto la Auditoría Superior, cuenta con un Sistema de Gestión de Seguridad de la Información, que en su manual en el punto 9.2 se implementa la realización de auditorías internas la cual verifica la implantación y eficacia del sistema (SGSI), el resultado de la auditoría debería mostrar el nivel de cumplimiento que se tiene respecto a las políticas y procedimientos del sistema y su apego con los requisitos legales, pudiendo ser estos internacionales, nacionales, estatales o contractuales, de esta manera este órgano de fiscalización local puede demostrar su alcance y apego a lo referido por la el artículo 33 fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados así como lo dispuesto por el artículo 32 VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Sistema de Gestión de Seguridad de la Información de la Auditoría Superior del Estado de Jalisco.

El Sistema de Gestión de Seguridad de la Información (SGSI), es un sistema que identifica los diversos activos (personas, hardware, software, documentos, etc.), para llevar a cabo un análisis de los riesgos a los que pueden estar expuestos y realizar acciones que permitan minimizar el impacto en caso de presentarse. Todo esto para garantizar la confidencialidad, la integridad y la disponibilidad de dichos activos.

Como Sistema de Gestión se han documentado políticas, procesos, procedimientos, protocolos, formatos y demás actividades a fin de poder ser auditados y llevar acciones correctivas, con la finalidad de tener un proceso de mejora continua.

- Gestionar las amenazas de la institución que puedan afectar el cumplimiento de los objetivos: esto implica la identificación, el análisis y el tratamiento de los riesgos.
- Permitir a la organización un enfoque al riesgo: esto implica conocer cuántos y cuáles pueden ser los riesgos y verificar su impacto en la operación de cada elemento operativo.
- Contar con criterios y políticas específicas que permitan minimizar las amenazas que pudieran presentarse e impactar a los objetivos, institucionales, tácticos y operativos.
- Garantizar que nuestra información mantenga su confidencialidad, su integridad y su disponibilidad, para su adecuada utilización.

Elementos relevantes:

- Política y objetivos de seguridad de la información.
- Políticas particulares. Partes interesadas.
- Comité de seguridad de la información.
- Representante de la alta dirección.

Programa General de Capacitación.

1. Acceso a la Información (Generalidades).
    a. Marco regulatorio.
    b. Acceso a la información como derecho humano.
    c. ¿Cuándo la información es publica? (definir la clasificación de la información: fundamental, reservada, confidencial, proactiva y focalizada.)
    d. Principio de máxima publicidad en el acceso a la información.
    e. ¿Cuáles son nuestras obligaciones como generadores de información?
    f. Infracciones y sanciones por no cumplir lo dispuesto en materia de acceso a la información.
2. Documento de seguridad de la ASEJ.
    a. Importancia del documento de seguridad de quienes manejan datos personales.
    b. Marco regulatorio.
    c. Contenido del documento de seguridad.
    d. ¿Por qué es obligatorio?
    e. Armonización del documento de seguridad con el Sistema de Gestión de Seguridad de la Información.
    f. Actualización del documento de seguridad cuando ocurran eventos que lo ameriten.
3. Protección de datos personales (Generalidades)
    a. Marco regulatorio
    b. Protección de datos personales como derecho humano.
    c. El documento de seguridad de la ASEJ como herramienta vinculatoria en la protección de datos personales.

d. Tratamiento adecuado de los datos personales en la institución en cuanto a la transferencia de los mismos.
e. Ejercicio de los derechos ARCO (Actualización, Rectificación, Cancelación y Oposición.)
f. Infracciones y sanciones por el incumplimiento en materia de protección de datos personales.

4. Versiones públicas.
    a. ¿Qué datos se deben suprimir en las versiones públicas y cuáles son los necesarios para dar mayor certeza jurídica del acto realizado?
    b. ¿Cómo se deben realizar las versiones públicas?
    c. ¿Cuándo se deben realizar versiones públicas?
    d. Lineamientos actualizados y autorizados por el ITEI para la realización de versiones públicas.
    e. Datos abiertos ¿Cuáles son los formatos de datos abiertos y fácil acceso?
5. Archivo
    a. Marco regulatorio.
    b. Obligatoriedad de la ASEJ como Sujeto Obligado.
    c. Infracciones administrativas y delitos en materia de archivos.
    d. Realización de Guía de archivo documental.
    e. Índice de expedientes clasificados como reservados
    f. Vinculación de la Ley General de Archivos y la Ley General de Transparencia y Acceso a la Información Pública.

Técnicas utilizadas para la supresión y borrado seguro de los datos personales

Los datos personales una vez que su ciclo de vida transcurriera según corresponda, a la finalidad por la cual fueron recabados, procederá a la supresión y borrado, durante dicho periodo no se podrán realizar acciones relativas al tratamiento de los mismos, procediendo de esta manera a la supresión de la base de datos, archivo o registro respectivo, se aplicara la normatividad archivística aplicable para la legal aplicación de esta técnica.

Se establece la documentación de los procedimientos que se utilizaran para la supresión y borrado de los datos personales que el responsable tiene en su poder, en el cual se incluirá los plazos de conservación si en su caso se requiriera, así como la realización de una revisión periódica sobre la necesidad de su conservación.

Catálogo de Sistemas de Tratamiento de Datos Personales.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Informes finales de la revisión de la cuenta pública realizada por la Auditoría Superior del Estado de Jalisco
Respecto del administrador de éste	nombre	Lic. María Teresa Arellano Padilla
	cargo	Auditora Especial de Cumplimiento Financiero
	adscripción	Auditoría Especial de Cumplimiento Financiero
Las funciones y obligaciones de las personas que traten datos personales		Atribuciones: Las descritas en el Reglamento Interno de la Auditoría Superior del Estado de Jalisco en sus artículos 11. Responsabilidades: Supervisar la ejecución de auditorías para verificar que los ingresos, incluyendo los captados por financiamientos, correspondan a los estimados y que fueron obtenidos, registrados y controlados de conformidad con la normatividad aplicable.
Inventario de los datos personales		De Funcionarios Públicos y o Beneficiarios en programas sociales: domicilio, clave de elector, CURP, RFC, Grupo sanguíneo y Factor RH, No. telefónico, Proveedores de los municipios si es persona física : Nombre de persona física o moral, RFC, domicilio, correo electrónico, cuenta bancaria, (comprobantes con requisitos fiscales presentados en las cuentas públicas municipales)
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Mecanismos: 1.-Es remitido por parte de la Dirección de Responsabilidades la documentación comprobatoria del informe mediante un memorándum.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vuleraciones a la seguridad de los datos personales		A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda, se levantará una bitacora de las vulneraciones con la fecha en que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informar en un plazo de 72 horas al Titular de los Datos, al encargado de la Unidad de Transparencia de la ASEJ y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Las enunciadas en el Sistema de Gestión de Seguridad de la Información
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	Respaldo. -Se resguarda los papeles de trabajo de las auditorías realizadas y los legajos de auditoría, de proveedores y de documentación solicitada, en el Archivo Semi-activo de la ASEJ a cargo de la Dirección General de Administración.
Plan de contingencia	Acciones Preventivas. -Las señaladas en el manual de Sistema de Gestión de Seguridad de la Información. Acciones Correctivas. - No aplica al no existir vulneraciones a esta fecha. PROPUESTA: Promover con el personal de la Dirección la cultura de la protección de datos personales, mediante la capacitación correspondiente para que conozcan sus alcances, así como las sanciones que se imponen a los infractores.
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	FISICAS: NINGUNA ELECTRONICAS: NINGUNA

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

PODER LEGISLATIVO	DOCUMENTO DE SEGURIDAD	
Nombre del sistema o base de datos		PROCEDIMIENTO DE ELABORACIÓN DEL PROYECTO DE INFORME FINAL DE AUDITORÍA DE LA ASEJ
Respecto del administrador de éste	**nombre**	Lic. José Antonio Delgadillo Madera
	cargo	Director de Responsabilidades
	adscripción	Dirección de Responsabilidades
Las funciones y obligaciones de las personas que traten datos personales		Atribuciones: Las descritas en el Reglamento Interno de la Auditoria Superior del Estado de Jalisco en su artículo 20 Responsabilidades: La elaboración del proyecto de informe final de auditoría que rinde la Auditoría Superior del Estado de Jalisco al Congreso del Estado, sobre la revisión de la cuenta pública y los estados financieros, el cual consiste en el cierre definitivo de la auditoría del ejercicio fiscal que corresponda Definir las actividades que se realizan en cada una de las áreas con la finalidad de recabar los
Inventario de los datos personales		De Funcionarios Públicos y o Beneficiarios en programas sociales: domicilio, clave de elector, CURP, RFC, Grupo sanguíneo y Factor RH, No. telefónico, (dependiendo del tipo de identificación oficial). Proveedores si es persona física, de los municipios: Nombre de persona física RFC, domicilio, correo electrónico, cuenta bancaria. (comprobantes con requisitos fiscales presentados en las cuentas públicas municipales))
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Mecanismos: 1.-Se remite por parte de las direcciones correspondientes la documentación comprobatoria del ente auditable por revisar, control de informes finales donde el auditor debe firmar de recibido. 2.-Se elabora el Proyecto de Informe Final de Auditoría y es turnado con la informacion al Despacho de la Auditora Especial de Cumplimiento Financiero
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vuleraciones a la seguridad de los datos personales		A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales. Se implementa el uso de la bitacora.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
NO APLICA Por el momento no se conoce que existan vulneraciones.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Medidas de seguridad físicas: Equipo de computo personal. Las enunciadas en el Sistema de Gestión de Seguridad de la Información
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	Respaldo. -Se resguarda los papeles de trabajo de las auditorias realizadas y los legajos de auditoría, de proveedores y de documentación solicitada, en el Archivo Semi-activo de la ASEJ a cargo de la Direccion General de Administración.Se resguarda los papeles de trabajo de las auditorías que se estan llevando a cabo así como los legajos de auditoría, de proveedores y de documentación solicitada, una bodega de la Auditoria Especial de Cumplimiento Financiero
Plan de contingencia	Acciones Preventivas. -Las señaladas en el manual de Sistema de Gestión de Seguridad de la Información. Acciones Correctivas. - No aplica al no existir vulneraciones a esta fecha. PROPUESTA: Promover con el personal de la Dirección la cultura de la protección de datos personales, mediante la capacitación correspondiente para que conozcan sus alcances, así como las sanciones que se imponen a los infractores.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Instrumento de satisfacción del cliente derivado de las auditorías realizadas por la Auditoria Superior del Estado de Jalisco
Respecto del administrador de éste	**nombre**	Soledad Rizo Orozco
	cargo	Auditora
	adscripción	Dirección de Programación, Evaluación y Seguimiento
Las funciones y obligaciones de las personas que traten datos personales		Recepción, revisión y resguardo de instrumentos de satisfacción del cliente aplicados a las y los sujetos auditados para medir el desarrollo de la auditoría y el desempeño del equipo auditor. Resguardo físico desde el 2015, resguardo electrónico 2010-2017
Inventario de los datos personales		firma de las y los sujetos auditados.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Los instrumentos se encuentran en un espacio restringido bajo, oficina bajo llave. Si se requiere consultar dichos instrumentos es necesario la autorización del titular del área. Apego a políticas particulares del Sistema de gestión de seguridad de la información (SGSI).
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		**Vulnerabilidades identificadas:** Todas las vulnerabilidades que se identificaron en la Matriz de administración de riesgos del SGSI (RC-PS-SI-006). A la fecha no se han materializado ningún riesgo, por tal motivo no se tiene registro de hechos. Se establece el uso de la bitacora.
Análisis de riesgos		
3		
Análisis de brecha		
4		
Gestión de vulneraciones		
Hasta el momento no se ha tenido vulneraciones, sin embargo, en caso de que suceda se realizará un registro de las vulneraciones con la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.		
Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones		a) Determinación de áreas seguras mediante la guía para la clasificación de documentos GI-PS-SI-01.Del sistema de gestion de Seguridad de la Información. b) Acceso del personal a las instalaciones vía tarjetas de proximidad, según actividades y políticas particulares del SGSI descritas en el Procedimiento para el ingreso a las diversas áreas de la institución PG-PS-SI-03. Del sistema de gestion de Seguridad de la Información. c) Acceso al personal visitante se realiza mediante el procedimiento para registrar al personal visitante PE-AD-RF-11. d) Control de vigilancia en las entradas y salidas del edificio.
Controles de identificación y autenticación de usuarios		5
Procedimientos de respaldo y recuperación de datos personales		No se tiene un respaldo, la documentación solo se conserva en físico.
Plan de contingencia		Acciones preventivas: ninguna. Acciones correctivas: atender las actividades descritas en el Procedimiento para implantar acciones correctivas PG-PS-GC-06

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		PROCEDIMIENTO DE REVISIÓN A LA CUENTA PÚBLICA MUNICIPAL EN TRABAJOS DE ESCRITORIO O GABINETE DE LA AUDITORÍA SUPERIOR DEL ESTADO DE JALISCO.
Respecto del administrador de éste	**nombre**	L.C.P. Salvador Sánchez Hernández.
	cargo	Director de Auditoria a Municipios
	adscripción	Dirección de Auditoría a Municipios
Las funciones y obligaciones de las personas que traten datos personales		Atribuciones: Las descritas en el Reglamento Interno de la Auditoria Superior del Estado de Jalisco en sus artículos 16, 17, 26, 27 y 28. Responsabilidades Solicitar y obtener toda la información y documentación necesaria para el cumplimiento de los trabajos de escritorio o gabinete, mediante la solicitud de la cuenta pública de la entidad auditable en el archivo general de la ASEJ a cargo de la DGA, así como llevar a cabo la integración de los expedientes correspondientes a los papeles de trabajo realizados durante la ejecución de los trabajos de escritorio o gabinete en la auditoria de la entidad auditable. .
Inventario de los datos personales		De Funcionarios Públicos y o Beneficiarios en programas sociales: domicilio, clave de elector, CURP, RFC, Grupo sanguíneo y Factor RH, No. telefónico ,etc. (dependiendo del tipo de identificación oficial). Proveedores de los municipios: Nombre de persona física o moral, RFC, domicilio, correo electrónico, cuenta bancaria, (comprobantes con requisitos fiscales presentados en las cuentas públicas municipales) etc.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Mecanismos: 1.-Se solicita al archivo semi-activo de la ASEJ, la cuenta pública del ente auditable por revisar, mediante un formato controlado con clave RC-AD-RF-005 de solicitud de préstamo de cuentas públicas municipales, mismo que es autorizado por el Director. 2.-Se regresa la cuenta pública a su lugar de resguardo que es el archivo semi-activo de la ASEJ a cargo de la Dirección General de Administración.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vuleraciones a la seguridad de los datos personales		A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se conoce que existan vulneraciones.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	"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. Las enunciadas en el Sistema de Gestión de Seguridad de la Información y en el PE-AM-AM-02.
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	proveedores y de documentación solicitada, en el Archivo Semi-activo de la ASEJ a cargo de la Dirección General de Administración
Plan de contingencia	Acciones Preventivas. -Las señaladas en el manual de Sistema de Gestión de Seguridad de la Información y en el PE-AM-AM-02 Acciones Correctivas. - No aplica al no existir vulneraciones a esta fecha. PROPUESTA: Promover con el personal de la Dirección la cultura de la protección de datos personales, mediante la capacitación correspondiente para que conozcan sus alcances, así como las sanciones que se imponen a los infractores.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		PROCEDIMIENTO DE REVISIÓN A LA CUENTA PÚBLICA MUNICIPAL EN TRABAJOS DE ESCRITORIO O GABINETE DE LA AUDITORÍA SUPERIOR DEL ESTADO DE JALISCO.
Respecto del administrador de éste	**nombre**	L.C.P. Salvador Sánchez Hernández.
	cargo	Director de Auditoria a Municipios
	adscripción	Dirección de Auditoría a Municipios
Las funciones y obligaciones de las personas que traten datos personales		Atribuciones: Las descritas en el Reglamento Interno de la Auditoria Superior del Estado de Jalisco en sus artículos 16, 17, 26, 27 y 28. Responsabilidades Solicitar y obtener toda la información y documentación necesaria para el cumplimiento de los trabajos de escritorio o gabinete, mediante la solicitud de la cuenta pública de la entidad auditable en el archivo general de la ASEJ a cargo de la DGA, así como llevar a cabo la integración de los expedientes correspondientes a los papeles de trabajo realizados durante la ejecución de los trabajos de escritorio o gabinete en la auditoria de la entidad auditable. .
Inventario de los datos personales		De Funcionarios Públicos y o Beneficiarios en programas sociales: domicilio, clave de elector, CURP, RFC, Grupo sanguíneo y Factor RH, No. telefónico, etc. (dependiendo del tipo de identificación oficial). Proveedores de los municipios: Nombre de persona física o moral, RFC, domicilio, correo electrónico, cuenta bancaria, (comprobantes con requisitos fiscales presentados en las cuentas públicas municipales) etc.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		**1**
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Mecanismos: 1.-Se solicita al archivo semi-activo de la ASEJ, la cuenta pública del ente auditable por revisar, mediante un formato controlado con clave RC-AD-RF-005 de solicitud de préstamo de cuentas públicas municipales, mismo que es autorizado por el Director. 2.-Se regresa la cuenta pública a su lugar de resguardo que es el archivo semi-activo de la ASEJ a cargo de la Dirección General de Administración.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		**2**
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se conoce que existan vulneraciones.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	"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. Las enunciadas en el Sistema de Gestión de Seguridad de la Información y en el PE-AM-AM-02.
Controles de identificación y autenticación de usuarios	**5**
Procedimientos de respaldo y recuperación de datos personales	proveedores y de documentación solicitada, en el Archivo Semi-activo de la ASEJ a cargo de la Dirección General de Administración
Plan de contingencia	Acciones Preventivas. -Las señaladas en el manual de Sistema de Gestión de Seguridad de la Información y en el PE-AM-AM-02 Acciones Correctivas. - No aplica al no existir vulneraciones a esta fecha. PROPUESTA: Promover con el personal de la Dirección la cultura de la protección de datos personales, mediante la capacitación correspondiente para que conozcan sus alcances, así como las sanciones que se imponen a los infractores.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Dirección de Auditoría a la Obra Pública
Respecto del administrador de éste	**nombre**	Ing. Ernesto Paredes Cárdenas
	cargo	Director
	adscripción	Dirección de Auditoría a la Obra Pública
Las funciones y obligaciones de las personas que traten datos personales		Instrumentar sistemas requeridos para la operación y funcionamiento de la Dirección de Auditoría a la Obra pública, que conlleven el cumplimiento de sus objetivos administrando los recursos materiales y humanos asignados y supervisando su optimización. Vigilar que durante el desempeño de sus funciones, en el espacio físico destinado para el resguardo de los datos personales, no tengan acceso a ellos personas no autorizadas. Se extraen datos personales en los siguientes procedimientos y documentos de la DAOP: Procedimiento para visita de campo o inspección, y en los documentos, Oficio de comisión (RC-AS-SP-003); acta de inicio de visita (RC-OP-JO-001), Expedientes técnico-administrativos, acta circunstanciada (RC-OP-JO-009), acta de cierre de visita (RC-OP-JO-002). PE-OP-OP-01 Procedimiento para el proyecto de pliego de observaciones y/o recomendaciones; pliego de observaciones municipal (RC-OP-JO-005), pliego de observaciones metropolitano (RC-OP-JO-006), pliego de observaciones ejecutivo (RC-OP-JO-007) pliego de recomendaciones (RC-OP-JO-008). PE-OP-OP-02 Procedimiento para el anteproyecto de informe final de auditoría; Se envía el anteproyecto de informe anexando la documentación aclaratoria, oficio(s) de comisión, actas de inicio de visita y cierre de visita de auditoria.
Inventario de los datos personales		edad, domicilio, colonia, entidad, código postal, tipo de identificación oficial, folio de identificación, firma, edad, RFC, CURP, teléfonopersonal , correo electrónico personal .
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		**1**
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		En auditorías, se realizan oficios y actas con información. Los formatos contiene datos personales con soportes físicos y son perceptible de cualquier violación. Se transfieren y reciben datos personales a Municipios, Entidades de Gobierno, Organismos Públicos Descentralizados y Autónomos Municipales
El resguardo de los soportes físicos y/o electrónicos de los datos personales		**2**
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		La o el Jefe del Departamento de EIES es responsable del monitoreo y la revisión de resultados de las bitácoras generadas que se indican en diversos documentos del SGSI, según lo establecido en la Política 88 del Sistema de Seguridad de la Información. Al día 09 de marzo de 2018 no se han presentado vulneraciones.

1 y 2, Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Dirección de Auditoría a la Obra Pública
Respecto del administrador de éste	**nombre**	Ing. Ernesto Paredes Cárdenas
	cargo	Director
	adscripción	Dirección de Auditoría a la Obra Pública

Análisis de riesgos
1

Análisis de brecha
2

Gestión de vulneraciones
por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda se levantará una bitácora de las vulneraciones con la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informa en un plazo de 72 horas al titular de los datos y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
Controles de identificación y autenticación de usuarios	**3**
Procedimientos de respaldo y recuperación de datos personales	Se deben realizar respaldos totales de los sistemas y bases de datos, los cuales deberán ser resguardados de acuerdo al procedimiento para el respaldo de información y de acuerdo a las políticas de respaldo del Sistema de Gestión de la Seguridad (P49 a la P54).
Plan de contingencia	Se asume el plan contenido en las Políticas Particulares del Sistema de Seguridad de la Información, que establece un plan de continuidad de operaciones basado en el tratamiento de riesgos, que permitan la continuidad de las operaciones de los procesos dentro del alcance de los Sistemas de Gestión de la Calidad y Seguridad de la Información, así como la protección de datos personales (P24).

1, 2 y 3 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Auditoría a la cuenta pública de los Poderes del Estado, Organismos Públicos Autónomos y al Sector Paraestatal. Base de datos: Archivos físicos y electrónicos, tanto de documentación generada en la DAPEOPA como de la remitida a la ASEJ por las entidades auditables, la obtenida durante la visita de auditoría y la proporcionada por terceros (proveedores, contratistas, respuesta a compulsas, beneficiarios de programas, entre otros).
Respecto del administrador de éste	nombre	Lic. Jorge Villanueva Jiménez
	cargo	Director de Auditoría a la cuenta pública de los Poderes del Estado, Organismos Públicos Autónomos y al Sector Paraestata
	adscripción	Dirección de Auditoría a la cuenta pública de los Poderes del Estado, Organismos Públicos Autónomos y al Sector Paraestatal
Las funciones y obligaciones de las personas que traten datos personales		Las funciones y obligaciones de las personas de la DAPEOPA que tratan datos personales se encuentran previstas en los artículos 16, 19, 26, 27 y 28 del Reglamento Interno de la Auditoría Superior del Estado de Jalisco, así como en lo previsto en los Procedimientos Específicos de la Dirección Procedimiento para la Planeación de la Auditoría, Procedimiento para el Desahogo de Procedimientos de Auditoría, Procedimiento para la Formulación de Pliegos de Observaciones y Recomendaciones, y Procedimiento para la Elaboración del anteproyecto de Informe Final y Anteproyecto de Informe del Resultado del Oficio de Recomendaciones.
Inventario de los datos personales		De Funcionarios y o Servidores Público • Domicilio, • Nacionalidad,• Registro Federal de Contribuyentes (RFC)• Clave Única de Registro de Población (CURP) • Número de registro a la seguridad social (IMSS o ISSSTE) • Lugar y fecha de nacimiento, • Edad,• Género,• Estado civil,• Tipo de sangre (factor RH• Número de cuenta bancaria,• Número telefónico, De proveedores y contratistas si son personas físicas: • Nombre, • Domicilio, • Nacionalidad,• Datos de alta en el Servicio de Administración Tributaria (SAT)• Registro Federal de Contribuyentes (RFC)• Clave Única de Registro de Población (CURP)• Lugar y fecha de nacimiento, • Género• Número de cuenta bancaria,• Número telefónico• Giro o actividad preponderante• Correo electrónico. Beneficiarios de programas sociales: • Nombre• Domicilio• Nacionalidad• Lugar y fecha de nacimiento• RFC• CURP• Género• Número de cuenta bancaria
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información y datos en forma electrónica se encuentran en dispositivos de almacenamiento (USB, CD's, DVD's) debidamente resguardados, así como respaldados en los equipos de cómputo del personal adscrito a esta Dirección. Una vez formulado en Anteproyecto de Informe Final y el Anteproyecto del Informe del Resultado del Oficio de Recomendaciones, el Expediente Continuo de Auditoría, el soporte documental de las observaciones y recomendaciones, la documentación aclaratoria a los pliegos de observaciones y recomendaciones proporcionada por los sujetos auditables, así como los archivos físicos y electrónicos, se remiten a la Dirección de Responsabilidades de la ASEJ. Las cédulas y papeles de trabajo (tanto impresas como los archivos electrónicos) se remiten mediante memorándum a la Dirección General de Administración para su debido resguardo en el Archivo de la Institución.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A la fecha no se conoce que existan vulneraciones a la seguridad de los datos personales. No obstante lo anterior, a efecto de evitar este riesgo, se implementarán los controles inherentes para garantizar la protección de datos personales en posesión del personal de esta Dirección.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda se levantará una bitácora de las vulneraciones con la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se informará en un plazo de 72 horas al titular de los datos y al ITEI. Lo anterior, de conformidad a lo establecido en los artículos 40 al 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Las medidas de seguridad físicas y electrónicas con que se cuenta al momento, son las previstas en el Sistema de Gestión de Seguridad de la Información (Política y objetivos de seguridad de la información y Políticas particulares), así como en los mecanismos establecidos en los Procedimientos Específicos de la Dirección que forman parte de nuestro Sistema de Gestión de la Calidad.
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	Se resguardan las cédulas, papelesde trabajo y demás documentación obtenida con motivo de la revisión a la auditoría de la cuenta pública de las entidades auditables por 6 meses
Plan de contingencia	Acciones Preventivas. -Las señaladas en el manual de Sistema de Gestión de Seguridad de la Información de esta institución. Plan de contingencia.- A la fecha no se cuenta con un plan de contingencia. Una vez que esta Dirección efectúe el análisis y matriz de riesgos, así como el análisis de brecha, se propondrá el Plan de Contingencia correspondiente.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Sistema Informático Estatal de Auditoría - Subsistema de control de Capacitación -ASEJ Sistema Integral e Información - Control de Capacitación
Respecto del administrador de éste	nombre	Mtra. Sofia Vázquez García
	cargo	jefa de departamento
	adscripción	Departamento de Profesionalización en la Fiscalización Superior
Las funciones y obligaciones de las personas que traten datos personales		Captura de listas de asistencia y puntos de capacitación en el Softw are arriba mencionado, aspi como análiis y vaciado de las cédulas de necesidades de capacitación, que contienen datos personales de las y los servidores públicos de la ASEJ.
Inventario de los datos personales		Correos electrónicos personales de quienes laboran en la ASEJ., RFC, dirección personal.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Los nombres de los servidores públicos , de la plantilla se envian vía correo electrónico a la Secretaria de Planeación, Administración y Finanzas y a la Auditoría Superior de la Federación, para la inscripción y capacitación ofrecidas por esas entidades
Procedimientos de respaldo y recuperación de datos personales		Resguardo físico, Archiveros. Resguardo electrónico en Sistema Informático Estatal de Auditoría, Subsistema de control de Capacitación, Sistema Integral de Información, Control de Capacitación y en carpeta de red denominada Profesionalización.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se identifican las vulnerabilidades señaladas en la Matriz de Administración de Riesgos del Sistema de Gestión de Seguridad de la Información (RC-PS-SI-006); sin embargo, a la fecha no se ha materializado ningún riesgo, por tal motivo no se tiene registro de algún, se implementa el uso de la bitacora.

1, 2, 3 y 4 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de riesgos
2

Análisis de brecha
3

Gestión de Vulnerabilidades
En caso de que suceda vulneración alguna, se levantará una bitácora con las vulneraciones en la que se especifique la fecha en la que ocurrieron, el motivo y las acciones que se implementaron para tal efecto, de esta misma manera se debe dar aviso al Titular de la Unidad de Transparencia de la ASEJ y al ITEI en un plazo de 72 horas.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13).
Controles de identificación y autenticación de usuarios	4
Procedimientos de respaldo y recuperación de datos personales	En relación a la documentación obtenida con motivo de la revisión, examen y fiscalización de la cuenta pública del Estado de Jalisco y sus Municipios; se observará el Procedimiento para respaldo de la información PE-TE-EI-08, así como las políticas de respaldo del Sistema de Gestión de Seguridad de la Información.
Plan de contingencia	Se observará el Procedimiento para implantar acciones correctivas PG-PS-GC-06. Así mismo y con la finalidad de lograr la proteccion de todo tipo de activo, el manetnimiento de la integridad de la información y el aseguramiento de su disponibilidad y de la protección de los datos personales, se realizará el Procedimeinto para la ejecucución del Plan de continuidad de operaciones PG-PS-SI-06.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos de los Servidores Públicos que cursan Diplomado en Materia de Área Gubernamental
Respecto del administrador de éste	**nombre**	Joaquin Javier Villa Martinez
	cargo	Jefe de Departamento
	adscripción	Departamento de Planeación Programación y Coordinación Técnica
Las funciones y obligaciones de las personas que traten datos personales		Entregar Diploma a los Servidores Públicos que acrediten el Diplomado en Materia del Área Gubernamental, recibiendo copia de identificación oficial
Inventario de los datos personales		Se cuenta con archivo electrónico y fisico de la relación del los Servidores Públicos que reciben Diploma. El archivo se integra además con una identificación oficial, y en su caso con una carta poder simple de quien recibe el diploma.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		No se realiza transferencia de datos
Procedimientos de respaldo y recuperación de datos personales		Se cuenta con expediente fisico resguardado en carpetas y bajo llave en archivero de la secretaria.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se identifican las vulnerabilidades señaladas en la Matriz de Administración de Riesgos del Sistema de Gestión de Seguridad de la Información (RC-PS-SI-006); sin embargo, a la fecha no se ha materializado ningún riesgo, por tal motivo no se tiene registro de algún

Análisis de riesgos
2

Análisis de brecha
3

Gestión de Vulnerabilidades
En caso de que suceda vulneración alguna, se levantará una bitácora con las vulneraciones en la que se especifique la fecha en la que ocurrieron, el motivo y las acciones que se implementaron para tal efecto, de esta misma manera se debe dar aviso al Titular de los datos personales , al encargado de la Unidad de Transparencia de la ASEJ al ITEI en un plazo de 72 horas.

Medidas de seguridad fisicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13). *Políticas para la operación de los activos (P14, P15, P16, P17, P18 y P19). *Políticas para el manejo de incidentes (P20, P21, P22 y P23). *Políticas de continuidad de operaciones (P24, P25, P26, P27 y P28). *Políticas de sistemas de información (P29, P30, P31 y P32). *Políticas de operación (P55, P56, P57, P58, P59, P60, P61, P62, P63, P64, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P84, P85, P86, P87, P88, P89, P90, P91, P92, P93, P94 y P95).
Controles de identificación y autenticación de usuarios	4
Procedimientos de respaldo y recuperación de datos personales	En relación a la documentación obtenida con motivo de la revisión, examen y fiscalización de la cuenta pública del Estado de Jalisco y sus Municipios; se observará el Procedimiento para respaldo de la información PE-TE-EI-08, así como las políticas de respaldo del Sistema de Gestión de Seguridad de la Información.
Plan de contingencia	Se observará el Procedimiento para implantar acciones correctivas PG-PS-GC-06. Así mismo y con la finalidad de lograr la proteccion de todo tipo de activo, el manetnimiento de la integridad de la información y el aseguramiento de su disponibilidad y de la protección de los datos personales, se realizará el Procedimeinto para la ejecucución del Plan de continuidad de operaciones PG-PS-SI-06.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Directorio Estatal, Municipal, Autónomos y Fideicomisos
Respecto del administrador de éste	**nombre**	Cristobal Zepeda Avila
	cargo	Encargado del Departamento de Capacitación a Entidades Fiscalizadas
	adscripción	Departamento de Capacitación a Entidades Fiscalizadas
Las funciones y obligaciones de las personas que traten datos personales		La base de datos es utilizada para realizar invitaciones a los cursos de capacitación a los servidores públicos estatales o municipales, mediante correo electrónico y via telefónica
Inventario de los datos personales		Se cuenta con base de datos de las autoridades del órden estatal y municipal, contando con los siguientes datos personales: Firma autógrafa de funcionarios públicos y correos electrónicos personales
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		No se realiza transferencia de datos
Procedimientos de respaldo y recuperación de datos personales		Se tiene archivo físico resguardado en carpetas y bajo llave en la oficina de jefatura y archivo electrónico en Excel en el equipo de cómputo resguardado por el Encargado de Capacitación.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se identifican las vulnerabilidades señaladas en la Matriz de Administración de Riesgos del Sistema de Gestión de Seguridad de la Información (RC-PS-SI-006); sin embargo, a la fecha no se ha materializado ningún riesgo, por tal motivo no se tiene registro de algún

1, 2, 3 y 4 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de riesgos
2

Análisis de brecha
3

Gestión de Vulnerabilidades
En caso de que suceda vulneración alguna, se levantará una bitácora con las vulneraciones en la que se especifique la fecha en la que ocurrieron, el motivo y las acciones que se implementaron para tal efecto, de esta misma manera se debe dar aviso al Titular de los datos personales y al ITEI en un plazo de 72 horas.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13).
Controles de identificación y autenticación de usuarios	4
Procedimientos de respaldo y recuperación de datos personales	En relación a la documentación obtenida con motivo de la revisión, examen y fiscalización de la cuenta pública del Estado de Jalisco y sus Municipios: se observará el Procedimiento para respaldo de la información PE-TE-EI-08, así como las políticas de respaldo del Sistema de Gestión de Seguridad de la Información.
Plan de contingencia	Se observará el Procedimiento para implantar acciones correctivas PG-PS-GC-06. Así mismo y con la finalidad de lograr la proteccion de todo tipo de activo, el manetnimiento de la integridad de la información y el aseguramiento de su disponibilidad y de la protección de los datos personales, se realizará el Procedimeinto para la ejecucución del Plan de continuidad de operaciones PG-PS-SI-06.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Catálogo de Proveedores de Capacitación
Respecto del administrador de éste	**nombre**	Mtra. Sofia Vázquez Garcia
	cargo	Jefa de Departamento
	adscripción	Departamento de Profesionalización en la Fiscalización Superior
Las funciones y obligaciones de las personas que traten datos personales		Solicitar información a empresas y/o instructores para la capacitación del personal de la ASEJ. Integrar las propuestas en el formato de autorización a proveedores y tramitar pagos de cursos a la Dirección Administrativa.
Inventario de los datos personales		Nombre, domicilio, teléfono, curriculum, RFC, datos bancarios para transferencias electrónicas, correo electrónico de los proveedores si son personas fisicas
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Se transfieren los datos a los proveedors vía electrónica y física a la Dirección General de Administración para su pago correspondiente.
Procedimientos de respaldo y recuperación de datos personales		Archivos electrónicos en la computadora de la Auditoría en comento y expedientes físicos en mobiliario bajo llave.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se identifican las vulnerabilidades señaladas en la Matriz de Administración de Riesgos del Sistema de Gestión de Seguridad de la Información (RC-PS-SI-006); sin embargo, a la fecha no se ha materializado ningún riesgo, por tal motivo no se tiene registro de algún o, se implementa el uso de la bitacora.

1, 2, 3 y 4 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de riesgos
2

Análisis de brecha
3

Gestión de Vulnerabilidades
En caso de que suceda vulneración alguna, se levantará una bitácora con las vulneraciones en la que se especifique la fecha en la que ocurrieron, el motivo y las acciones que se implementaron para tal efecto, de esta misma manera se debe dar aviso al Titular de los datos personales, al ITEI y al encargado de la Unidad de Transparencia en un plazo de 72 horas.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13).
Controles de identificación y autenticación de usuarios	4
Procedimientos de respaldo y recuperación de datos personales	En relación a la documentación obtenida con motivo de la revisión, examen y fiscalización de la cuenta pública del Estado de Jalisco y sus Municipios; se observará el Procedimiento para respaldo de la información PE-TE-EI-08, así como las políticas de respaldo del Sistema de Gestión de Seguridad de la Información.
Plan de contingencia	Se observará el Procedimiento para implantar acciones correctivas PG-PS-GC-06. Así mismo y con la finalidad de lograr la proteccion de todo tipo de activo, el manetnimiento de la integridad de la información y el aseguramiento de su disponibilidad y de la protección de los datos personales, se realizará el Procedimeinto para la ejecucución del Plan de continuidad de operaciones PG-PS-SI-06.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Información del personal que integra la Unidad Interna de Protección Civil (UIPC) de la Auditoría Superior del Estado de Jalisco.
Respecto del administrador de éste	**nombre**	Roberto Alejandro Fernández Hernández
	cargo	Supervisor
	adscripción	Dirección de Programación, Evaluación y Seguimiento
Las funciones y obligaciones de las personas que traten datos personales		Llevar el control de la información del personal que integra la UIPC de la ASEJ.
Inventario de los datos personales		Nombre, domicilio particular, teléfono de casa y celular, sexo, tipo de sangre y aspectos de salud (alergias, enfermedades o discapacidades) de los brigadistas
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		**1**
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La base de datos se encuentra en una carpeta dentro de una oficina bajo llave. Apego a políticas particulares del Sistema de gestión de seguridad de la información (SGSI) sobre el manejo e intercambio de información. La base de datos se encuentra en el equipo de cómputo con password de acceso del Supervisor de la Doctora de la ASEJ.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		**2**
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		**Vulnerabilidades identificadas:** Todas las vulnerabilidades que se identificaron en la Matriz de administración de riesgos del SGSI (RC-PS-SI-006). A la fecha no se han materializado ningún riesgo, por tal motivo no se tiene registro de hechos. Se implementa el uso de la bitacora.
Análisis de riesgos		
3		
Análisis de brecha		
4		
Gestión de vulneraciones		
Hasta el momento no se ha tenido vulneraciones, sin embargo, en caso de que suceda se realizará un registro de las vulneraciones con la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.		
Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones		a) Determinación de áreas seguras mediante la guía para la clasificación de documentos GI-PS-SI-01. Del sistema de gestion de Seguridad de la Información. b) Acceso del personal a las instalaciones via tarjetas de proximidad, según actividades y políticas particulares del SGSI descritas en el Procedimiento para el ingreso a las diversas áreas de la institución PG-PS-SI-03. Del sistema de gestion de Seguridad de la Información. c) Acceso al personal visitante se realiza mediante el procedimiento para registrar al personal visitante PE-AD-RF-11. d) Control de vigilancia en las entradas y salidas del edificio.
Controles de identificación y autenticación de usuarios		**5**
Procedimientos de respaldo y recuperación de datos personales		Se cuenta con un respaldo en la red que atiende al procedimiento para el respaldo de información PE-TE-EI-08 y las políticas particulares del SGSI que ahí se describen.
Plan de contingencia		Acciones preventivas: ninguna. Acciones correctivas: atender las actividades descritas en el Procedimiento para implantar acciones correctivas PG-PS-GC-06

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

PODER LEGISLATIVO		DOCUMENTO DE SEGURIDAD
Nombre del sistema o base de datos		Área médica de la Auditoría Superior del Estado de Jalisco
Respecto del administrador de éste	nombre	Lic. Mario Alberto Manzano Luna
	cargo	Jefe de la Unidad de Recursos Humanos
	adscripción	Dirección General de Administración
Las funciones y obligaciones de las personas que traten datos personales		Área encargada de la plantilla del personal de la ASEJ, de los expedientes médicos de los mismos y del área de registro de visitantes.
Inventario de los datos personales		Información sensible de servidores públicos de la ASEJ: Nombre, Edad, Estado Civil, Fecha de nacimiento, Domicilio, Puesto, Teléfono particular, Nombre y teléfono de dos familiares, Número de Seguro Social, Número de afiliación de seguro de gastos médicos mayores, Tipo de sangre, Peso y estatura, Antecedentes heredo-familiares, Antecedentes patológicos, Antedentes de alergias, transfusiones, tabaquismo, alcoholismo, Antecedentes ginecológicos, Antecedentes prostáticos, Agudeza auditiva y Condición odontológica
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		No existe transferencia de datos, en caso de que un paciente sea remitido a otra clínica, consultorio y/o hospital, solamente se informa los síntomas que presentó el paciente y medicamentos que hayan administrado previamente.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Hasta la fecha no se cuenta con bitácoras de acceso.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda, se levantará una bitacora de las vulneraciones con la fecha en que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informar en un plazo de 72 horas al Titular de los Datos y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13). *Políticas para la operación de los activos (P14, P15, P16, P17, P18 y P19). *Políticas para el manejo de incidentes (P20, P21, P22 y P23). *Políticas de continuidad de operaciones (P24, P25, P26, P27 y P28). *Políticas de sistemas de información (P29, P30, P31 y P32). *Políticas de operación (P55, P56, P57, P58, P59, P60, P61, P62, P63, P64, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P84, P85, P86, P87, P88, P89, P90, P91, P92, P93, P94 y P95).
Controles de identificación y autenticación de usuarios	Físico: Los expedientes médicos los tiene la Doctora en un archivero con llave, solamente ella tiene acceso. Electrónico: la computadora de la Doctora tiene contraseña.
Procedimientos de respaldo y recuperación de datos personales	5
Plan de contingencia	Plan de contingencia.- A la fecha no se cuenta con un plan de contingencia. Una vez que esta Dirección efectúe el análisis y matriz de riesgos, así como el análisis de brecha, se propondrá el Plan de Contingencia correspondiente

PODER LEGISLATIVO

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Departamento de Recursos Humanos de la Auditoria Superior del Estado de Jalisco
Respecto del administrador de éste	**nombre**	Mario Alberto Manzano Luna
	cargo	Jefe de la Unidad de Recursos Humanos
	adscripción	Dirección General de Administración
Las funciones y obligaciones de las personas que traten datos personales		Área encargada de la plantilla del personal de la ASEJ, de los expedientes médicos de los mismos y del área de registro de visitantes.
Inventario de los datos personales		Inventario de datos personales de los servidores públicos de la ASEJ: Comprobante de domicilio, Identificación oficial, Certificado médico, Certificado de estudios, Acta de nacimiento, fotografia.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Únicamente los transfieren entre unidades de la ASEJ, pero se necesita la autorización del trabajador para revisar su expediente.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A la fecha no se cuenta con bitácoras de acceso.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda, se levantará una bitacora de las vulneraciones con la fecha en que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informar en un plazo de 72 horas al Titular de los Datos, al Encargado de la Unidad de Transparencia de la ASEJ y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13). *Políticas para la operación de los activos (P14, P15, P16, P17, P18 y P19). *Políticas para el manejo de incidentes (P20, P21, P22 y P23). *Políticas de continuidad de operaciones (P24, P25, P26, P27 y P28). *Políticas de sistemas de información (P29, P30, P31 y P32). *Políticas de operación (P55, P56, P57, P58, P59, P60, P61, P62, P63, P64, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P84, P85, P86, P87, P88, P89, P90, P91, P92, P93, P94 y P95).
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	Actualmente se están escaneando los documentos para tener los documetos en formato digital.
Plan de contingencia	Plan de contingencia.- A la fecha no se cuenta con un plan de contingencia. Una vez que esta Dirección efectúe el análisis y matriz de riesgos, así como el análisis de brecha, se propondrá el Plan de Contingencia correspondiente

PODER LEGISLATIVO

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Unidad Centralizada de Compras de la Auditoría Superior del Estado de Jalisco
Respecto del administrador de éste	**nombre**	Itzel Sánchez Torres
	cargo	Jefa de la Unidad Centralizada de Compras
	adscripción	Dirección General de Administración
Las funciones y obligaciones de las personas que traten datos personales		Área encargada de compras, solicita datos personales a los proveedores.
Inventario de los datos personales		Proveedores registrados como personas físicas: Nombre, Comprobante de domicilio, RFC, Identificación oficial vigente, Número de cuenta,Acta de nacimiento.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		1
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Solamente se transfieren internamente a Juridico para revisión de los contratos y a la unidad de contabilidad.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		2
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Hasta la fecha no se cuenta con bitácoras de acceso

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda, se levantará una bitacora de las vulneraciones con la fecha en que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informar en un plazo de 72 horas al Titular de los Datos, al encargado de la Unidad de Transparencia y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13). *Políticas para la operación de los activos (P14, P15, P16, P17, P18 y P19). *Políticas para el manejo de incidentes (P20, P21, P22 y P23). *Políticas de continuidad de operaciones (P24, P25, P26, P27 y P28). *Políticas de sistemas de información (P29, P30, P31 y P32). *Políticas de operación (P55, P56, P57, P58, P59, P60, P61, P62, P63, P64, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P84, P85, P86, P87, P88, P89, P90, P91, P92, P93, P94 y P95).
Controles de identificación y autenticación de usuarios	5
Procedimientos de respaldo y recuperación de datos personales	Se realizan respaldos por medio del programa KÓRIMA.
Plan de contingencia	Plan de contingencia.- A la fecha no se cuenta con un plan de contingencia. Una vez que esta Dirección efectúe el análisis y matriz de riesgos, así como el análisis de brecha, se propondrá el Plan de Contingencia correspondiente

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Registro del ingreso al inmueble de la ASEJ
Respecto del administrador de éste	**nombre**	Lic. Mario Alberto Manzano Luna
	cargo	Jefe de la Unidad de Recursos Humanos
	adscripción	Dirección General de Administración
Las funciones y obligaciones de las personas que traten datos personales		Área encargada de la plantilla del personal de la ASEJ, de los expedientes médicos de los mismos y del área de registro de visitantes.
Inventario de los datos personales		Nombre de las personas externas a la ASEJ, Identificación oficial, foto de la persona y/o foto de la identificación.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		**1**
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		Se transfieren los datos del registro a la unidad de informática y de ahí a Recursos Humanos quienes son los responsables del área de Registro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		**2**
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Hasta la fecha no se cuenta con bitácoras.

1, 2, 3 4 y 5 Se eliminaron por considerarse información confidencial según lo dispuesto por el artículo 17. 1 de la Ley de Transparencia y Acceso a la Información pública del Estado de Jalisco y sus Municipios.

Análisis de riesgos
3

Análisis de brecha
4

Gestión de vulneraciones
Por el momento no se han sufrido vulneraciones, sin embargo, en caso de que suceda, se levantará una bitacora de las vulneraciones con la fecha en que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva. Además se debe informar en un plazo de 72 horas al Titular de los Datos, al encargado de la Unidad de Transparencia de la ASEJ y al ITEI.

Medidas de seguridad físicas y electrónicas aplicadas a las instalaciones	Políticas Particulares del sistema de Gestión de Seguridad de la Información: * Políticas para el manejo e intercambio de información (P1, P2,P3, P4 y P5). *Políticas para el acceso y permanencia en el edificio (P6, P7, P8, P9, P10, P11, P12 y P13). *Políticas para la operación de los activos (P14, P15, P16, P17, P18 y P19). *Políticas para el manejo de incidentes (P20, P21, P22 y P23). *Políticas de continuidad de operaciones (P24, P25, P26, P27 y P28). *Políticas de sistemas de información (P29, P30, P31 y P32). *Políticas de operación (P55, P56, P57, P58, P59, P60, P61, P62, P63, P64, P65, P66, P67, P68, P69, P70, P71, P72, P73, P74, P75, P76, P77, P78, P79, P80, P81, P82, P83, P84, P85, P86, P87, P88, P89, P90, P91, P92, P93, P94 y P95).
Controles de identificación y autenticación de usuarios	**5**
Procedimientos de respaldo y recuperación de datos personales	Se cuenta con una base de datos protegida para evitar perder los registros.
Plan de contingencia	A la fecha no se cuenta con un plan de contingencia. Una vez que esta Dirección efectúe el análisis y matriz de riesgos, así como el análisis de brecha, se propondrá el Plan de Contingencia correspondiente