SEAJAL
Sistema Estatal Anticorrupción de Jalisco
Secretaría Ejecutiva

Política General de Seguridad de la Información de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco

Tabla de contenido

1. Información general

1.1. Introducción

La información corresponde a un activo, el cual se expone a riesgos y amenazas dinámicos que pueden provocar pérdidas materiales y económicas, daños en la imagen institucional y en la confianza del público en general, infracciones legales e incumplimiento regulatorio.

Establecer un Sistema de Gestión de Seguridad de la Información (SGSI)[1] ayudará a que los riesgos de la seguridad de la información, dentro de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco (SESAJ), sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible y eficiente.

Las Políticas de Seguridad de la Información son una parte del SGSI y están basadas en la norma internacional ISO 27001:2013, en la norma mexicana NMX-I-27001-NYCE-2015 y en el Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicación y de Seguridad de la Información (MAAGTICSI)[2].

1.2. Objetivo

Conservar la confidencialidad, integridad y disponibilidad de los activos de información que gestiona la SESAJ, a través del establecimiento de una Política General de Seguridad de Información (PGSI) que abonen al establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI).

1.3. Marco Normativo

Artículo 18 fracción III del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco.

[1] Un Sistema de Gestión para la Seguridad de la Información (SGSI), en inglés: *Information Security Management System*, (ISMS) consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen como objetivo la protección de los activos de información en una organización. El término es utilizado principalmente en la familia ISO/IEC 27000, desarrollada y publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para facilitar un marco reconocido de forma mundial a las prácticas de gestión de la seguridad de la información.

[2] https://periodicooficial.jalisco.gob.mx/sites/periodicooficial.jalisco.gob.mx/files/01-14-17-vi.pdf
MAAGTICSI es considerado por la SESAJ como parte de buenas prácticas esto en razón que su alcance se limita a la administración pública.

Políticas y Disposiciones para el Gobierno Digital del Gobierno de Jalisco, en materia de Tecnologías de la Información y Comunicación, así como Manual Administrativo de Aplicación General de dicha materia (MAAGTICSI), publicado en el Periódico Oficial del Estado de Jalisco el 14 de enero de 2017.[2]

1.4. Alcance

Estas políticas aplicarán a toda la información generada, obtenida, transformada, administrada, resguardada o en posesión de la SESAJ, por lo que serán de observancia obligatoria para el personal adscrito a la SESAJ y terceros que accedan a dicha información.

Los lineamientos, procedimientos, directrices y guías desarrolladas a partir de estas políticas deben aplicarse en todas las fases del ciclo de vida de la información: generación, distribución, almacenamiento, procesamiento, transporte, acceso, consulta y destrucción; para todos los sistemas, infraestructuras tecnológicas y las instalaciones que los soportan.

1.5. Definiciones

Concepto	Definición
Activo de información	Sistemas de información y demás información o equipos, incluyendo documentos en papel, equipos portátiles, soportes de almacenamiento de datos, etc.
Amenaza	Todo elemento o acción, que aprovecha una vulnerabilidad y que es capaz de atentar contra la seguridad de la información.
Áreas seguras	Son sitios en los que se maneja información sensible o que contienen equipos informáticos valiosos para la institución.
Borrado seguro	El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
BYOD	Trae tu propio dispositivo, por sus siglas en inglés Bring Your Own Device, tendencia en creciente aumento que permite a los servidores públicos utilizar sus dispositivos tecnológicos personales para desarrollar funciones laborales.
Confidencialidad	Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos legalmente autorizados.
Controles	Medidas, mecanismos o acciones utilizadas para verificar, evaluar y aumentar la seguridad de la información.
Disponibilidad	Es la capacidad de que la información permanezca accesible en el sitio, en el momento y en la forma en que los usuarios que estén autorizados la requieran.
Dispositivos tecnológicos personales	Se refiere equipos personales (computadoras portátiles, teléfonos inteligentes, tabletas, memorias USB, cámaras digitales, etc.) propiedad de los servidores públicos y visitantes, utilizados dentro de las instalaciones de la SESAJ.
Impacto	Grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.
Infraestructura Tecnológica	Todos los elementos físicos o lógicos que son requeridos para brindar los servicios y soluciones informáticas, tales como: Centros de datos, cuartos de equipo, cuartos de telecomunicaciones, equipos y redes de comunicación de voz y datos, servidores de cómputo, equipos auxiliares de cómputo y comunicaciones, software adquirido o desarrollado por SESAJ, sistemas operativos, manejadores de bases de datos.

Integridad	Es la cualidad que posee un documento que no ha sido alterado y que además permite comprobar que el documento es original. La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
Jailbreak	Proceso mediante el cual se superan las restricciones de un dispositivo con Sistema Operativo iOS, permitiendo tener acceso al administrador y cambiar la configuración del sistema operativo.
Política General de Seguridad de la Información	Conjunto de medidas, reglas, controles y protocolos de actuación esenciales en materia de seguridad de la información.
Riesgo	Es la posibilidad de que ocurra un evento que afecte adversamente el logro de los objetivos de la SESAJ. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.
Roles	Conjunto de responsabilidades, actividades y autorizaciones que se otorgan a una persona o equipo. Una persona o equipo pueden tener varios roles.
Rooteo	Operación que consiste en elevar los permisos de usuario a administrador en dispositivos móviles con sistema operativo Android, con el propósito de realizar operaciones avanzadas y potencialmente peligrosas.
Seguridad de la información	Es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad de la organización y minimizar los riesgos.
Sistema de Gestión de Seguridad de la Información	Un sistema de Gestión de Seguridad de la Información (SGSI), en inglés: *Information Security Management System*, (ISMS) consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen como objetivo la protección de los activos de información en una organización. El término es utilizado principalmente en la familia ISO/IEC 27000, desarrollada y publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para facilitar un marco reconocido de forma mundial a las prácticas de gestión de la seguridad de la información.
Vulnerabilidad	Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta.

1.6. Acrónimos

Acrónimo	Descripción
ACL	Access Control List – Lista de Control de Acceso
DTP	Dirección de Tecnologías y Plataformas de la SESAJ
ERISC	Equipo de respuesta a incidentes de seguridad en TIC en la SESAJ
GESI	Grupo Estratégico de Seguridad de la Información
GSI	Gerencia de Seguridad de la Información
IPS	Intrusion Prevention System – Sistema de Prevención de Intrusos
MAAGTICSI	Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicación y de Seguridad de la Información. Es considerado por la SESAJ como parte de buenas prácticas esto en razón que su alcance se limita a la administración pública.
NAS	Network Attached Storage – Almacenamiento conectado en red
OIC	Órgano Interno de Control
RSII	Responsable de la Seguridad de la Información Institucional
SEAJAL	Sistema Anticorrupción del Estado de Jalisco
SESAJ	Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Jalisco
SGSI	Sistema de Gestión de Seguridad de la Información
TI - TICs	Tecnologías de Información y Comunicación
VPN	Virtual Private Network – Red Privada Virtual

1.7. Roles y Responsabilidades

Responsable de la Seguridad de la Información en la Secretaría Ejecutiva (RSII)

- La responsabilidad principal de promover la seguridad de la información recae en la figura del Secretario Técnico
- Revisa este documento
- Hace del conocimiento de la Política General de Seguridad de la Información ante el Órgano de Gobierno de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción

Gerencia de Seguridad de la Información (GSI)

- Rol del Director de Tecnologías y Plataformas de la SESAJ
- Gestiona la actualización de estas políticas
- Elabora propuestas de modificaciones y mejores a las presentes políticas
- Coordina la revisión y actualización del presente documento cuando se requiera o derive de:
  - Alguna modificación al marco jurídico y normativo aplicable
  - Observaciones y/o recomendaciones por parte de instancias de supervisión y fiscalización, así como, del Órgano de Gobierno de la SESAJ o de las autoridades competentes.
- Es responsable de asegurar la alineación operativa de TIC con las políticas establecidas
- Debe asegurar que las contrataciones relacionadas con TIC cuenten con cláusulas que promuevan el cumplimiento de estas políticas

Grupo Estratégico de Seguridad de la Información (GESI)

- Integrado por el Director de Tecnologías y Plataformas de la SESAJ; el Subdirector de Operación de Servicios; el Subdirector de Desarrollo de Sistemas y Soluciones y el Subdirector de Proyectos Tecnológicos; un representante de la Unidad de Transparencia; un representante de la Unidad de Inteligencia de Datos y un representante de la Coordinación Administrativa.
- Da visto bueno al documento
- Propone mejoras
- Se aseguran de cumplir y hacer cumplir las políticas establecidas
- Deben conocer, y dar a conocer las políticas establecidas
- Proporciona apoyo especializado al personal de la SESAJ
- Sugiere modificaciones o adhesiones a este documento.

Órgano Interno de Control (OIC)

- Revisa el documento en apego a los Objetivos y Lineamientos del Sistema de Control Interno de SESAJ
- Promueve la transparencia y el apego a los principios de legalidad, honradez, lealtad, imparcialidad y eficiencia de los servidores públicos mediante el ejercicio de sus atribuciones.
- Atiende, tramita y en su caso, resuelve las denuncias presentadas contra presuntas irregularidades administrativas cometidas por los servidores públicos de la SESAJ

Propietarios de activos de información

- Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo
- Cada miembro del personal tiene la responsabilidad de no revelar indebidamente información confidencial

2. Políticas

2.1. Políticas Generales

1. Es responsabilidad de todos los participantes de la SESAJ conocer, cumplir y hacer cumplir las disposiciones de esta Política.
2. Esta política podrá ser revisada al menos una vez al año, y cuando ocurran cambios significativos que lo ameriten.
3. La información es un activo que tiene valor para la SESAJ y por consiguiente debe ser debidamente protegida.
4. Cada Dirección, Coordinación y demás Unidades Administrativas deben elaborar y mantener un inventario de los activos de información que poseen.
5. Todo el personal de la SESAJ debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI.

2.2. Seguridad en los Recursos Humanos

Previas al nombramiento o designación

La Coordinación Administrativa, a través de la Jefatura de Recursos Humanos, es la responsable del resguardo de la información referente a los cuestionarios de evaluación y entrevista(s) que puede(n) incluir evaluaciones prácticas que en su caso realice con motivo de la designación o nombramiento del personal de la SESAJ y dentro del marco de sus atribuciones.

La Coordinación Administrativa, a través de la Jefatura de Recursos Humanos, debe dar a conocer y recabar la firma del personal de la SESAJ, del acuerdo de confidencialidad de la información.

Durante la relación laboral

Es responsabilidad de la Coordinación Administrativa informar a todo el personal de nuevo ingreso de la existencia de estas Políticas Generales de Seguridad de la Información; las cuales deberán ser firmadas de forma autógrafa además de guardar una copia en el expediente personal para el caso de responsabilidades o vulneraciones.

La Coordinación Administrativa debe incluir como parte de la inducción al personal de nuevo ingreso, el material informativo necesario sobre la seguridad de la información.

Es responsabilidad de los coordinadores, jefes de unidad, subdirectores y directores de la SESAJ, promover y hacer del conocimiento a todo personal a su cargo de la existencia de estas Políticas Generales de Seguridad de la Información.

Es responsabilidad de los coordinadores, jefes de unidad, subdirectores y directores de la SESAJ, promover en todo momento, la participación en los procesos de concientización, capacitación y prevención a incidentes de seguridad, a todo el personal a su cargo, con el fin de fortalecer una cultura de la información.

Todo personal de la SESAJ debe reportar por correo electrónico o documento impreso, a la Gerencia de Seguridad de la Información, cualquier falta u omisión de las Políticas Generales de Seguridad de la Información. La Gerencia de Seguridad de la Información debe notificar al Responsable de la Seguridad de la Información, para que, de acuerdo con la gravedad, informe al Órgano Interno de Control para que en el ámbito de su competencia resuelva lo conducente.

Terminación o separación del puesto

Toda terminación de las relaciones laborales o de servicios, según sea el caso, debe apegarse a los procesos involucrados de la Coordinación Administrativa, la Jefatura de Recursos Humanos, la Dirección de Tecnologías y Plataformas y demás relacionadas, promoviendo que la separación del puesto sea de una manera ordenada, disminuyendo así el riesgo hacia los activos de información propiedad de la SESAJ.

La Dirección de Tecnologías y Plataformas, a través de la Subdirección de Operación de Servicios, debe notificar de forma oportuna al superior jerárquico del personal que termina dichas relaciones, la afectación de la inhabilitación de su(s) cuenta(s), lo anterior para disminuir riesgos en la operación de la SESAJ.

La Coordinación Administrativa encabezará los trabajos para establecer un proceso de desvinculación de personal, que incluirá el alcance y detalle de las actividades que se deben realizar cuando un recurso humano termina su relación laboral o de servicios con la SESAJ.

Toda terminación o separación del puesto deberá sujetarse al Proceso de respaldo de información, devolución de activos informáticos e inhabilitación de cuentas institucionales, establecido por la Dirección de Tecnologías y Plataformas.

2.3. Gestión de los activos

Se entiende como activo de información los sistemas de información y demás información o equipos, incluyendo documentos en papel, equipos portátiles, soportes de almacenamiento de datos, etc. Con las siguientes características:

- Es valioso para la SESAJ por la información que contiene
- Es derivado o es el producto del ejercicio de las funciones o atribuciones encomendadas.
- No es de fácil remplazo y en algunos casos puede ser irrepetible
- Tiene valor administrativo, legal o contable

Inventario de activos

Es responsabilidad de los coordinadores, jefes de unidad, subdirectores y directores de la SESAJ identificar sus activos de información.

La Dirección de Tecnologías y Plataformas debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios TIC de SESAJ.

El GESI debe coordinar la identificación de los activos esenciales de la SESAJ y promover la protección de estos activos.

Propiedad de los activos

Toda información que se genere a partir de un activo propio, arrendado o contratado por un servicio, es propiedad de la SESAJ.

Todo activo de información debe ser asignado a un responsable y autorizado por su jefe inmediato.

La persona responsable del activo debe:

1. Salvaguardar la integridad, disponibilidad y confidencialidad del activo.
2. Hacer uso del activo únicamente para los propósitos y actividades de la SESAJ.
3. Reportar, a la Dirección de Tecnologías y Plataformas, cualquier incidente o problema relacionado con el activo de la información.

4. Cualquier omisión, con dolo o involuntariamente, de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información.
5. Realizar lo necesario para mantener el activo de información en buenas condiciones que garantice y cumpla su función.

Todos los aplicativos y sistemas institucionales que soporten algún proceso, deben tener un responsable funcional de un área de la SESAJ y ser integrados por la Dirección de Tecnologías y Plataformas, a su catálogo de servicio.

La Dirección de Tecnologías y Plataformas debe proveer los recursos necesarios, así como las herramientas tecnológicas que ayuden a fortalecer la seguridad lógica y física de la información del activo, así como el resguardo del licenciamiento correspondiente.

Uso aceptable de los activos

La SESAJ considera que los recursos para el procesamiento de la información son prioritarios para el desarrollo y adecuado cumplimiento de sus funciones; por lo que, es responsabilidad del personal, el salvaguardar de cualquier alteración o modificación no autorizada, daño o destrucción que límite su disponibilidad para el adecuado desarrollo de sus actividades.

El uso aceptable de los activos de información incluye:

1. Evitar daños temporales o permanentes a los activos de información, causados por accidentes, imprudencias o daños dolosos.
2. Reportar cualquier falla o mal funcionamiento detectado.
3. Informar a los jefes inmediatos, de cualquier falla o vulnerabilidad de los activos de información.
4. Notificar de cualquier necesidad de protección o mejora, en los controles para los activos de información.
5. Usar los activos de información únicamente para los propósitos de la SESAJ.
6. Reportar cualquier uso no adecuado del activo de información a su jefe inmediato.

Devolución de los activos

Todo personal que preste sus servicios a la SESAJ, al concluir sus funciones, tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

La entrega – recepción de los activos informáticos debe apegarse a los procedimientos establecidos por la SESAJ, a lo establecido en el artículo 48.1 fracción X, de la Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco y los artículos 1, 9, 11 y demás relacionados de la Ley de Entrega - Recepción del Estado de Jalisco y sus Municipios.

2.4. Clasificación de la información

Directrices de clasificación

Cada área debe clasificar y etiquetar su información de acuerdo con la Ley General de Transparencia y Acceso a la Información Pública; la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; la Ley General de Archivo; la Ley de Archivos del Estado de Jalisco y sus municipios; el reglamento interno de transparencia y acceso a la información pública de la Secretaría Ejecutiva del Sistema Anticorrupción de Jalisco; así como observar los lineamientos generales en materia de clasificación de información pública, previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y los lineamientos generales en materia de clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas.

La información debe clasificarse como:

1. **Información pública**

   Es toda información que generen, posean o administren los sujetos obligados, como consecuencia del ejercicio de sus facultades o atribuciones, o el cumplimiento de sus obligaciones, sin importar su origen, utilización o el medio en el que se contenga o almacene; la cual está contenida en documentos, fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático, holográfico o en cualquier otro elemento técnico existente o que surja con posterioridad. *Artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.*

La información pública se clasifica, según el artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, en:

I) Información pública de libre acceso
II) Información pública protegida
III) Información proactiva
IV) Información focalizada

2. **Información reservada**
   Es la información creada y usada por la SESAJ, en la realización de sus procesos, que corresponda a lo dispuesto en los artículos 17, 18 y 19 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

3. **Información confidencial**
   Es la información creada y usada por la SESAJ, en la realización de sus procesos, que corresponde a lo dispuesto en los artículos 20, 21, 21 Bis, 22, y 23 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Su divulgación externa debe estar en apego a los términos de las disposiciones aplicables.

Todas las áreas de la SESAJ tienen la obligación de designar un enlace en materia de transparencia, quien será responsable al interior de su área, de coordinarse y apoyar a la Unidad de Transparencia de la SESAJ, para dar cumplimiento puntual a los diferentes requerimientos en la materia.

Etiquetado de la información

El Comité de Transparencia de la SESAJ, entre otras atribuciones, será quien deba confirmar, modificar o revocar las determinaciones que, en materia de clasificación de la información realicen los titulares de las áreas administrativas de la SESAJ, de acuerdo con lo establecido en el artículo 30.1 fracción II de Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus municipios.

Lo anterior, mediante, un análisis fundado y motivado para la clasificación de la información pública, en el que se observe lo previsto en los artículos 60, 61, 62, 63, 63bis, 64 y 65 de la Ley citada en el párrafo anterior, el cual deberá remitir para su revisión y consideración el área generadora y/o poseedora de la información al Comité de Transparencia de la SESAJ a través de su Unidad de Transparencia.

El etiquetado de la información se aplicará en apego a lo establecido en la Ley de Archivos del Estado de Jalisco y sus municipios, en los catálogos de etiquetado establecidos por el área de archivo de la SESAJ y demás legislación aplicable.

Protección y manejo de la información

La Dirección de Tecnologías y Plataformas debe proveer mecanismos de protección de la información, de acuerdo con su clasificación.

Todo activo de información protegido según su clasificación debe contar con un control de acceso, donde se establezca qué personas son las autorizadas para el manejo de la información en el activo.

Los servidores públicos de la SESAJ, están obligados a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.

Los usuarios de acuerdo con sus funciones podrán trabajar y hacer uso de la información de la SESAJ en los activos de información asignados y resguardar la versión final.

Protección de datos personales

En materia de protección de datos personales, se deberá cumplir lo dispuesto con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; así como observar los Lineamientos Generales en materia de clasificación de información pública, previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Las áreas de la SESAJ deberán de justificar todo tratamiento de datos personales que efectúen, con un fin concreto, lícito, explícito y legítimo, relacionado con las atribuciones que la normatividad le aplique.

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, las áreas de la SESAJ deberán considerar y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales,

que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como cuidar su confidencialidad, integridad y disponibilidad.

Para lo anterior, se deberán atender las medidas y procedimientos establecidos por la Unidad de Transparencia de la SESAJ, incluido el documento de seguridad de la SESAJ, el cual contiene las disposiciones en materia de protección de datos personales de las unidades administrativas de este Ente, dicho instrumento 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, lo anterior con fundamento en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y del artículo 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

2.5. Seguridad física y del entorno

El objetivo de este apartado es asegurar que sólo los usuarios autorizados tengan acceso a las instalaciones de procesamiento de información, esto para prevenir cualquier daño físico o interferencia con los equipos o las instalaciones.

Áreas seguras

La Dirección de Tecnologías y Plataformas en conjunto con la Coordinación Administrativa establecerán y designarán las áreas seguras de la SESAJ.

Las áreas seguras son espacios físicos que albergan activos de información y/o equipos de procesamiento y almacenamiento de datos y que cuentan con acceso limitado a personal autorizado.

No se permitirá el acceso a las áreas seguras a personal que no esté expresamente autorizado.

En caso de que se autorice a un externo el acceso al área segura, éste deberá estar acompañado en todo momento de personal del área responsable de la SESAJ.

Control físico de entrada

Las áreas seguras deben contar con mecanismos de ingreso que consideren la autorización, registro y validación de los accesos.

Seguridad de oficinas, despachos y recursos

La Coordinación Administrativa debe proporcionar a cada empleado, un espacio físico asignado que cuente con mobiliario protegido para el resguardo de activos de información, incluyendo información física.

La Coordinación Administrativa debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo con sus funciones dentro de la SESAJ, el acceso a áreas restringidas debe ser autorizado por el área responsable del área restringida.

Protección contra amenazas externas y ambientales

La Coordinación Administrativa debe facilitar los recursos necesarios para establecer perímetros de seguridad física con el fin de proteger áreas que contengan información crítica de la SESAJ, así como el área de procesamiento de datos.

Los perímetros de seguridad física deben estar definidos e identificados.

Manejo de medios de almacenamiento

Gestión de medios removibles

Se entiende por medios removibles todo soporte o dispositivo de almacenamiento, independientes de la computadora y que pueden ser transportados libremente, fueron diseñados para ser extraídos de la computadora sin tener que apagarla. Ejemplos: discos ópticos, tarjetas de memoria, memorias USB, discos duros externos.

Los medios removibles no son alternativa de respaldo de información de la SESAJ, siendo responsabilidad del usuario almacenar y mantener la información en la nube o NAS institucional asignada por la Dirección de Tecnologías y Plataformas.

Los usuarios deben ser cuidadosos al utilizar dispositivos móviles y medios de almacenamiento removibles en lugares públicos, salas de reuniones y otras áreas fuera de la SESAJ.

Se deberá implementar medidas de protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos. Estas medidas pueden ser: protección de archivos con clave, huella digital, encriptado de la información almacenada o el mecanismo que permita el dispositivo.

En caso de pérdida o robo de activos de información, incluyendo medios removibles, el usuario afectado debe informar a la Dirección de Tecnologías y Plataformas y a la Coordinación Administrativa para tomar las medidas pertinentes.

Eliminación de medios

La Dirección de Tecnologías y Plataformas debe contar con procedimientos para asegurar la baja y el borrado confiable de los activos informáticos.

Los medios removibles deben ser formateados por personal de la Subdirección de Operaciones de Servicios, cuando la información pierda vigencia de acuerdo con la Política de eliminación o reutilización segura de equipos que establezca dicha subdirección.

Debe aplicarse un procedimiento de migración, respaldo y borrado seguro a todo activo informático que contenga información de la SESAJ, antes de que el activo sea eliminado o dado de baja.

2.6. Control de accesos

El objetivo de este apartado es asegurar que sólo usuarios autorizados accedan a los servicios de información de la SESAJ y que lo hagan a través de privilegios adecuados a su perfil o rol.

Política de control de acceso

La Dirección de Tecnologías y Plataformas debe establecer controles de seguridad para la Gestión de Cuentas de Usuarios en la SESAJ.

Los controles de acceso a los servicios de información deben asignarse con base en los roles y perfiles de los usuarios, según el servicio requerido.

La autenticación de usuarios debe hacerse a través de canales cifrados y haciendo uso de contraseñas encriptadas.

Gestión del acceso a usuarios

Gestión de altas/bajas/cambios en el registro de usuarios

Todo aplicativo y servicios de TIC de la SESAJ deben contar con un registro de altas, bajas y cambios de cuentas de usuarios, y seguir lo dispuesto en la Política de Gestión de Cuentas de usuarios establecidas por la Subdirección de Operaciones de Servicios.

Gestión de los derechos de acceso asignados a usuarios

Todos los accesos a servicios TIC y aplicativos deben ser asignados de acuerdo a sus funciones, mediante roles y perfiles, propiciando una correcta segregación de funciones.

Gestión de derechos de acceso con privilegios especiales

Los usuarios con privilegios especiales de acceso deben contar con la autorización del responsable del activo.

Gestión de información confidencial de autenticación de usuarios

La Dirección de Tecnologías y Plataformas o cualquier área de la SESAJ en posesión o manejo de cuentas de usuario, deben asegurar la confidencialidad en la entrega de contraseñas en todos sus procesos.

Revisión de los derechos de acceso de usuarios

Los derechos de acceso de los usuarios deben ser revisados anualmente por la Subdirección de Operaciones de Servicios y validados por cada área de la SESAJ.

Retirada o adaptación de los derechos de acceso

Es responsabilidad de la Coordinación Administrativa, con apoyo de la Jefatura de Recursos Humanos, notificar las bajas o cambios de adscripción del personal, a la Dirección de Tecnologías y Plataformas, para la ejecución del cambio o remoción de los derechos de acceso.

Es responsabilidad de los coordinadores, jefes de unidad, subdirectores y directores de la SESAJ que cuenten con personal externo, que tengan acceso a los servicios TIC y a los aplicativos

institucionales, notificar las bajas o cambios de funciones del personal, a la Dirección de Tecnologías y Plataformas, para la ejecución del cambio o remoción de los derechos de acceso.

Responsabilidades de los usuarios

Uso de información confidencial para la autenticación

Todo personal de la SESAJ es responsable de su contraseña, la cual es confidencial y debe mantenerse secreta.

Para hacer uso de la infraestructura tecnológica de la SESAJ, los usuarios deben aceptar los términos y condiciones de la Política de Uso Aceptable de Aplicativos y Servicios Tecnológicos Institucionales de la SESAJ.

El usuario debe cambiar la contraseña inicial, después de que le fue asignada al sistema aplicativo, mismo que debe estar configurado para que esto sea de forma automática.

Solo deben tener acceso a los aplicativos institucionales los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente o de otra persona.

2.7. Seguridad de los equipos

Todo equipo que almacene, procese o transmita información esencial para la operación de la SESAJ, debe ser protegido para disminuir riesgos de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo, etc.

La SESAJ debe contar con un cuarto principal de equipos o centro de datos primario que garantice la protección de activos de información y equipos que soportan los procesos institucionales, así como los servicios de soporte.

Además, la SESAJ debe contar con un almacenamiento y/o respaldo de datos o activos de información secundario, cuya ubicación geográfica sea distinta del cuarto principal de equipos o centro de datos primario, que garantice la continuidad de las operaciones, ante una contingencia.

Los cuartos de equipo deben cumplir con los estándares mínimos para la protección física y ambiental, por lo menos contar con:

- Señalización adecuada de todos los equipos y elementos de seguridad.
- Sistema de aire acondicionado configurados en la temperatura idónea para el correcto funcionamiento de los equipos y prevenir fallas.
- Sistemas de alimentación eléctrica ininterrumpida (UPS), redundante.
- Alarmas de detección de humo y/o sistemas automáticos de extinción de fuego.
- Extintores y equipos contra incendio con capacidad de detener el fuego generado por equipo eléctrico.
- Contar con control de acceso físico sólo para personal autorizado.

Seguridad en cableado

El cableado debe cumplir con las especificaciones del fabricante para minimizar errores físicos. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

Todo el cableado de datos debe estar debidamente etiquetado en los paneles de parcheo y adecuadamente instalado, para facilitar su mantenimiento.

Cuando exista un cambio en el cableado, se debe actualizar la memoria técnica correspondiente.

El cableado de datos y de energía debe estar separado en distintas canaletas o ductos, para evitar interferencias, siguiendo las normas aplicables.

El acceso a los espacios donde residan los paneles de parcheo y tableros de distribución eléctrica, debe ser restringido al personal responsable de la red y del soporte técnico o mantenimiento de estos.

Mantenimiento de los equipos

Todo activo de información debe contar con programas de soporte y mantenimiento, para su correcto funcionamiento y disponibilidad.

La Dirección de Tecnologías y Plataformas debe validar que los mantenimientos que se lleven a cabo sean realizados por personal capacitado, de acuerdo con las especificaciones del fabricante. Asimismo, asegurarse que se lleve un registro de todos los mantenimientos preventivos y correctivos efectuados.

Salida de equipos y activos

La Coordinación Administrativa debe establecer un procedimiento para el registro de entrada y salida de equipos de cómputo y activos de información de la SESAJ.

Seguridad de los equipos y activos fuera de las instalaciones

Todo equipo que almacene, procese o transmita información crítica de la SESAJ debe operar dentro de las instalaciones de la institución.

Los equipos o activos de información que por necesidad salgan de las instalaciones de la SESAJ, deben apegarse al procedimiento de salida de equipos establecido por la Coordinación Administrativa.

Los equipos de cómputo móviles (laptop) de la SESAJ deben ser protegidos con las medidas y mecanismos de seguridad de la información, con los que cuente la institución.

Los equipos de cómputo de la SESAJ que se encuentren fuera de las instalaciones y requieran conectarse a la red interna de la SESAJ, deberán realizarlo por medio del cliente VPN, siguiendo las Políticas establecidas por la Subdirección de Operación de Servicios.

Política de escritorio seguro y bloqueo de pantalla

La Dirección de Tecnologías y Plataformas debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática en un tiempo máximo de 5 minutos, una vez que éste se encuentre desatendido.

Todo el personal que preste sus servicios dentro de la SESAJ debe cumplir con los siguientes lineamientos al ausentarse de su lugar de trabajo o finalizar su jornada laboral:

- En caso de contar con puerta, cajones o archiveros, se deben cerrar con llave.
- Retirar del escritorio cualquier tipo de información, sin importar el medio en que se encuentre (papel, notas adhesivas, discos, memorias extraíbles) y resguardarla en gabinetes con llave o cualquier otro lugar con acceso controlado.
- Destruir de manera segura aquella información que ya no será utilizada apegándose a la normativa aplicable.
- No dejar documentos con información sobre impresoras, copiadoras, en el buzón de impresión, etc.

- No utilizar hojas con información impresa que sea confidencial o reservada como papel de reciclaje.

Uso de dispositivos tecnológicos personales en la SESAJ

Los servidores públicos que para el desempeño de sus labores decidan por cuenta propia, utilizar dispositivos tecnológicos personales, son directamente responsables de la información que almacenen, procesen o transfieran con esos elementos, quedando su consentimiento expreso para llevar a cabo revisiones de los dispositivos y dar cumplimiento de forma obligatoria a estas Políticas de Seguridad de la Información.

Todo dispositivo tecnológico personal será revisado por la Subdirección de Operación de Servicios antes de conectarlo por primera vez a la red de datos de la SESAJ; además podrá ser revisado en cualquier momento.

La Dirección de Tecnologías y Plataformas debe llevar un inventario de los dispositivos tecnológicos personales que se integren o hagan uso de la red de datos de la SESAJ.

Todos los dispositivos tecnológicos personales deberán tener configurado el bloqueo de pantalla por contraseña o patrón, esto con el fin de evitar accesos no autorizados al equipo e información que contienen.

Para poder autorizar la conexión del equipo a la red de datos de la SESAJ, el dispositivo tecnológico personal deberá de tener instalado una aplicación de tipo antivirus, firewall o cortafuegos activado y aplicar todas las actualizaciones del sistema operativo.

La Dirección de Tecnologías y Plataformas no está obligada a brindar soporte técnico a dispositivos tecnológicos personales.

Queda prohibido cualquier modificación o manipulación del sistema operativo del dispositivo tecnológico personal, esto incluye *rooteo* o *jailbreak*. Los dispositivos que hayan pasado por procedimientos de este tipo serán incluidos en una lista negra para evitar el acceso a la red de datos de la SESAJ.

El acceso a internet para dispositivos tecnológicos personales se proporcionará por la Dirección de Tecnologías y Plataformas, con los accesos y privilegios estrictamente indispensables para el desempeño de las actividades institucionales.

No se deberá almacenar información de la SESAJ en los dispositivos tecnológicos personales, en su lugar, se deberá configurar el almacenamiento directo en la nube.

Al finalizar la relación laboral de la persona servidor público con la SESAJ, la Dirección de Tecnologías y Plataformas realizará una revisión final a todo dispositivo tecnológico personal con el fin de evitar fuga de información. Además, se deberá aplicar un procedimiento de borrado seguro de la información institucional que se encuentre en el dispositivo.

Dispositivos móviles y teletrabajo

Es responsabilidad del personal, proteger los equipos que se le han asignado para el desempeño de sus funciones siguiendo las medidas de seguridad que a continuación se describen, como mínimo:

- No exponer el equipo a condiciones de inseguridad física y/o ambiental.
- Proteger las claves de acceso que le han sido asignadas
- No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado con relativa facilidad, como autos, maletas de viaje, cerca de ventanas, en el piso, mesas de comida, entre otros.
- Todo equipo asignado es de uso exclusivo del personal de SESAJ por lo que no deberá ser compartido o prestado a familiares y/o amigos.

Los usuarios que hagan uso de su dispositivo móvil personal para apoyar sus labores deben tomar los resguardos que estén a su alcance para asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada en el móvil.

2.8. Política de seguridad en las operaciones

Este apartado tiene por objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información que se procesa mediante los distintos mecanismos de comunicación y operación de los sistemas de información.

Protección contra código malicioso

La Dirección de Tecnologías y Plataformas debe asegurar que todos los equipos de escritorio, móviles y servidores utilizados en la red de la SESAJ, tengan habilitado, ya sea instalado en el equipo o de forma centralizada, software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware; además de mantenerlo actualizado, tanto en versión de sistema como en definición de firmas.

Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de la SESAJ, deben contar con software de antivirus. La Dirección de Tecnologías y Plataformas podrá verificar el correcto funcionamiento del equipo y reservar el derecho de acceso de equipos externos a la red de la SESAJ.

El software de antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional debe permitir como mínimo:

1- Ejecutar búsqueda automática, manual o programable.
2- Limpiar archivos infectados.
3- Mantener en cuarentena los archivos que no puedan ser limpiados.
4- Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.
5- Proveer la capacidad de actualizaciones automáticas y programables.
6- Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
7- Detectar código malicioso.
8- Generar alertas.
9- Llevar una administración centralizada.

La Dirección de Tecnologías y Plataformas debe establecer un repositorio de reportes mensuales que detallen las incidencias detectadas por el antivirus, en caso de no haber detectado incidencias deberá mencionarlo en el reporte.

Respaldo y borrado de la información

Respaldo de información

Todos los coordinadores, jefes de unidad, subdirectores y directores de la SESAJ, son responsables de identificar la información que sea sensible para la operación de su área de acuerdo con su

criticidad y deben notificar a la Dirección de Tecnologías y Plataformas para gestionar su respaldo y periodicidad.

La Dirección de Tecnologías y Plataformas debe:

1. Implementar procedimientos para respaldar la información de la SESAJ.
2. Respaldar periódicamente toda la información (configuraciones, registros, sistemas de archivo, bases de datos, etc.) que resida en los sistemas de la SESAJ, considerando su criticidad.
3. Asegurar que el respaldo de la información de los sistemas, en lo posible no degrade su operación.
4. Notificar, con al menos 24 horas de anticipación, cuando se requiera realizar respaldo que afecte la operación del servicio.
5. Preferentemente, realizar los respaldos fuera de los horarios de operación
6. Proveer espacios suficientes para almacenamiento y resguardo de la información de la organización que será respaldada periódicamente, siendo responsabilidad de cada usuario el manejo de la información a respaldar.
7. Revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que se cumple con los principios de integridad y disponibilidad.
8. Evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.
9. Almacenar los respaldos generados en un sitio protegido contra el medio ambiente y con controles estrictos de acceso.
10. Mantener un registro actualizado, con acceso controlado, que contenga los datos de los archivos respaldados, fuera de las instalaciones de la institución, indicando la fecha más reciente en que la información fue modificada.

Restauración e integridad

La Dirección de Tecnologías y Plataformas debe implementar medidas y procedimientos para promover la integridad y disponibilidad de la información de la SESAJ que sea respaldada.

La Dirección de Tecnologías y Plataformas debe:

1. Garantizar que los respaldos no sean alterados

2. Garantizar la integridad, disponibilidad y confidencialidad de los respaldos por lo menos tres años, desde su último respaldo
3. Realizar pruebas programadas y documentadas de restauración de información simulando situaciones de contingencia, en donde se revise la integridad y funcionalidad de los respaldos de información

Almacenamiento de información

La Dirección de Tecnologías y Plataformas debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su información institucional. Asimismo, debe contar con un inventario de usuarios autorizados en los recursos de almacenamiento de cada área.

Queda prohibido la utilización de recursos de almacenamiento institucional para archivos de uso personal o de diversión.

La Dirección de Tecnologías y Plataformas debe contar con procedimientos y mecanismos de borrado de la información de la institución, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

En caso de que se considere que existe información que ya no sea utilizada, se debe notificar a la Dirección de Tecnologías y Plataformas, para que, de manera coordinada con el Grupo Interdisciplinario de Archivo de la SESAJ, se determine si se puede eliminar de forma segura y de acuerdo con los criterios que establezcan las áreas responsables de la información.

Registro de actividad

Registro de eventos

Todos los sistemas y aplicaciones críticos de la SESAJ, bases de datos y dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente.

La Dirección de Tecnologías y Plataformas debe resguardar por un periodo de al menos tres años todos los registros de incidentes, alarmas, cambios, configuraciones, entre otros.

Sincronización de reloj

Todos los equipos de cómputo, sistemas, servidores, bases de datos y de comunicaciones que se encuentren en la red de la SESAJ, deben estar sincronizados con una fuente común y exacta de tiempo (servidor NTP).

La Dirección de Tecnologías y Plataformas debe implementar y documentar procedimientos para que los cambios de horario no afecten la operación de la SESAJ.

Control de software en sistemas operacionales

Instalación de software

La Dirección de Tecnologías y Plataformas debe contar con procedimientos para la validación del software que sea instalado. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo cuenten con el licenciamiento vigente, suficiente para atender los requerimientos de la organización.

La Dirección de Tecnologías y Plataformas es responsable de administrar y resguardar las licencias del software institucional.

Todo el software que se instale en ambientes productivos debe ser previamente evaluado y probado en ambientes de pruebas. La instalación del software autorizado debe ser realizado por personal calificado.

Todo el software que se instale en los equipos de cómputo debe estar inventariado en un catálogo de software institucional, realizado y actualizado por la Subdirección de Operaciones de Servicios.

Es responsabilidad de la Dirección de Tecnologías y Plataformas la adquisición del software requerido por las áreas de la SESAJ.

La Dirección de Tecnologías y Plataformas es la única instancia autorizada por la SESAJ para instalar, actualizar y desinstalar el software de los equipos de cómputo.

Queda prohibido al personal no autorizado, instalar y/o ejecutar software para explorar (escanear) redes, equipos de cómputo y sistemas de información, en busca de protocolos, puertos, recursos compartidos y vulnerabilidades; así como, el descubrimiento y monitoreo no autorizado del tráfico

de la red de la SESAJ. La Dirección de Tecnologías y Plataformas debe implementar mecanismos para restringir la instalación de software no autorizado.

2.9. Seguridad en las comunicaciones

El objetivo de este apartado es el de asegurar la protección de la información en las redes dentro de la SESAJ.

Gestión de seguridad de red

La Dirección de Tecnologías y Plataformas es responsable del diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan.

La Dirección de Tecnologías y Plataformas debe implementar procedimientos y controles tecnológicos para asegurar la integridad, disponibilidad y confidencialidad de la información, en su transmisión de las redes e infraestructuras de comunicaciones de la SESAJ.

La Dirección de Tecnologías y Plataformas debe establecer los requerimientos técnicos para la conexión a la red y sus servicios.

La SESAJ debe contar con la infraestructura necesaria para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

La Dirección de Tecnologías y Plataformas debe implementar mecanismos para el uso del servicio de internet de la SESAJ, el cual debe contar con herramientas de seguridad y de filtrado de contenido, que permitan la segmentación de navegación conforme a la operación de las áreas y roles o perfiles de usuarios.

Seguridad de los servicios de red

La Dirección de Tecnologías y Plataformas debe implementar:

a) Mecanismos que midan y aseguren los niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de los procesos de la SESAJ.
b) Medidas de control que aseguren la protección y confidencialidad de la información, generada por la SESAJ

Segregación en las redes

La administración e infraestructura de red debe estar clasificada en zonas de seguridad, basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento.

Se debe utilizar mecanismos de autenticación y cifrado para la protección de la comunicación inalámbrica.

Requerimientos de seguridad

La Dirección de Tecnologías y Plataformas debe cuidar el cumplimiento de los requerimientos de seguridad mínimos para cada elemento de la red de la SESAJ, entre ellos:

- Establecer controles de seguridad de acuerdo con el tipo zona de red
  - Firewall
  - Sistema de Prevención de Intrusiones (IPS)
  - Servidor de VPN
  - Servidor de autenticación de dominio
  - Filtrado de contenidos en la navegación hacia internet
  - Listas de Control de Acceso (ACL), en ruteadores y switches
- Encriptar la información confidencial que se transmita en la red.
- Monitoreo regular de los equipos y dispositivos de red, con el fin de identificar de manera oportuna problemas de desempeño e incidentes de seguridad.
- Correcta configuración de dispositivos de red, se deberán cambiar las contraseñas por defecto en estos dispositivos.
- El cableado de red voz y datos debe cumplir con las especificaciones del fabricante.

2.10. Transferencia de información

Políticas y procedimientos de transferencia de información

Se deberán establecer políticas y procedimientos de operación para la distribución y balanceo del tráfico en los enlaces de red principales de la SESAJ, considerando disponibilidad, confidencialidad, criticidad y redundancia.

Los recursos de red de la SESAJ no deben ser utilizados para propósitos personales, específicamente:

1. No está permitido descargar o intercambiar archivos no relacionados con información institucional, entre ellos música, video e imágenes de internet, en cualquier medio y desde cualquier medio, sólo se autorizará en caso de que la SESAJ o la actividad específica lo justifique.
2. Dentro de la red de la SESAJ, no está permitido conectar a internet equipos personales o servidores de red a no ser que sea previamente autorizado por el Secretario Técnico a través de la Dirección de Tecnologías y Plataformas.
3. Se prohíbe el acceso a blogs, redes sociales, páginas de entretenimiento, juegos, deportes, pornografía, música, videos, contenido violento, religión y cualquier otro contenido, no relacionado con las actividades de la SESAJ, salvo autorización del Secretario Técnico a través de la Dirección de Tecnologías y Plataformas y previa solicitud del responsable del área a la que pertenece el equipo requirente.
4. El Secretario Técnico y la Dirección de Tecnologías y Plataformas son las instancias con la autoridad para permitir monitorear el tráfico de la red. Este monitoreo se debe efectuar solamente con la finalidad de detectar anomalías, fallas o actividades sospechosas, los informes deben estar disponibles para el Responsable de la Seguridad de la Información.
5. Será sancionado cualquier uso comercial de los recursos y servicios de red e internet con fines diferentes a los institucionales.
6. Está prohibido descargar programas de internet "no autorizados" o sin licencia de uso institucional.

Acuerdos sobre la transferencia de información

Todas las áreas de la SESAJ que tenga intercambio de información con cualquier entidad externa, pública o privada, deben establecer acuerdos de privacidad específicos para la transferencia de información; además deberán contar con un inventario o bitácora de transferencias.

Los acuerdos de intercambio de información que se establezcan deben considerar como mínimo los siguientes aspectos:

- Acuerdos sobre etiquetado de la información
- Definición del medio de transporte para la transferencia de la información
- Canales autorizados para la transferencia de la información
- Definición de responsabilidades por divulgación o pérdida de información
- Acuerdos de privacidad específicos

Mensajería electrónica

La Dirección de Tecnologías y Plataformas debe cuidar la disponibilidad y confiabilidad del correo institucional.

El personal de la SESAJ está obligado a utilizar de forma adecuada los servicios de red y el servicio de correo institucional.

La Dirección de Tecnologías y Plataformas debe implementar políticas para la administración del correo electrónico institucional, que garanticen la trazabilidad y el no repudio.

La Dirección de Tecnologías y Plataformas tiene la facultad de suspender el servicio de correo electrónico institucional a la persona que haga mal uso.

No está permitido el uso del correo electrónico de la SESAJ para:

- Difundir cadenas de correos
- Difundir mensajes de discriminación racial, religiosa o política
- Difundir mensajes que promocionen negocios personales o particulares

Las únicas cuentas de correo autorizadas para el envío de mensajes de correo masivo son aquellas que por la naturaleza de sus funciones en la SESAJ hayan sido creadas con este propósito específico.

Los usuarios deben notificar a la Dirección de Tecnologías y Plataformas, para que, de manera coordinada con el Comité de Transparencia de la SESAJ, se analice la situación particular y en su caso borrar, sin abrir, los correos electrónicos que procedan de cuentas de correo que les sean desconocidas o sospechosas, así como aquellos cuyo "asunto" pueda relacionarse con publicidad, virus o SPAM.

No deben borrarse los mensajes de correo electrónico institucional esto porque pueden formar parte de la evidencia en los casos de auditorías y para temas de acceso a la información pública en materia de transparencia.

No debe hacerse uso de mensajería instantánea (Whatsapp, Telegram, Messenger) o redes sociales, para compartir información de operaciones o información confidencial.

Toda información recibida, transmitida y almacenada en los servidores de correo electrónico de la SESAJ se considera información de la institución.

Todos los correos electrónicos que se emitan desde cuentas de correo de la SESAJ deben contener la siguiente leyenda:

> *El contenido de este correo electrónico es información pública y susceptible de una solicitud de información.*
> Existe la posibilidad de que este correo electrónico contenga datos personales, que de acuerdo con lo establecido en el artículo 3, fracciones IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como información confidencial, de conformidad al artículo 21 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
>
> En ese tenor y atendiendo a lo establecido por el artículo 72 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, el receptor de los datos personales deberá tratar los mismos, comprometiéndose a garantizar su confidencialidad y únicamente utilizarlos para los fines que le fueron transferidos, además de que adquiere el carácter de responsable. El tratamiento de esta información deberá cumplir en todo momento con las disposiciones de las leyes antes señaladas, por lo que cualquier transferencia o tratamiento de los datos por personas o entidades distintas a las dirigidas se encuentra prohibido, salvo las excepciones previstas en los artículos 15 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Confidencialidad o acuerdos de no revelación

La Coordinación de Administración es responsable de establecer y mantener actualizado el contenido de todos los acuerdos de confidencialidad y de no revelación de información, que debe incluirse en los contratos, tanto para personal interno como para proveedores, según su área de competencia

2.11. Gestión de incidentes en la seguridad de la información

Este apartado tiene por objetivo establecer los lineamientos mínimos para gestionar los incidentes de seguridad de la información.

Responsabilidades y procedimientos

La SESAJ, a través del Responsable de la Seguridad de la Información Institucional (RSII), de acuerdo con el MAAGTICSI, debe establecer un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), definir roles y responsabilidades de los integrantes, asimismo, dar a

conocer las reglas de operación del mismo y la guía técnica de atención a incidentes a los participantes.

El ERISC debe estar conformado por personal de SESAJ con conocimientos técnicos y operativos de la infraestructura de la institución.

El ERISC es responsable de elaborar y dar mantenimiento al procedimiento para la respuesta a incidentes de seguridad, el cual debe ser avalado por el GESI.

El ERISC debe conocer los procedimientos de respuesta a incidentes, que considera al menos las etapas de:

1. Identificación y reporte
2. Contención
3. Recuperación
4. Solución
5. Lecciones aprendidas

El ERISC debe coordinar las acciones para solucionar los incidentes que afecten los servicios de información, para la operación de la SESAJ, en corresponsabilidad con las áreas afectadas e involucradas en la operación.

Los procedimientos para la notificación de incidentes deben estar fácilmente accesibles para todos los usuarios.

Informar eventos de seguridad de la información

La Dirección de Tecnologías y Plataformas debe notificar de forma inmediata al RSII, de todos los incidentes o amenazas detectados que puedan causar la degradación en los niveles de servicios acordados, en las infraestructuras catalogadas como esenciales de SESAJ.

Es responsabilidad de todo el personal de SESAJ reportar a la Dirección de Tecnologías y Plataformas los incidentes de seguridad de la información que tengan una probabilidad de materializar un riesgo.

De forma enunciativa, más no limitativa:

1. Accesos físicos no autorizados
2. Accesos lógicos no autorizados
3. Negación o degradación de servicios a sistemas de información
4. Recepción de correo basura (SPAM)
5. Robo de información
6. Incumplimiento a las políticas de seguridad de la información
7. Falla en la identificación o etiquetado de la información
8. Ataques de virus
9. Incumplimiento con leyes sobre protección de datos personales

Monitoreo e informes sobre puntos débiles de seguridad de la información

La Dirección de Tecnologías y Plataformas debe realizar el monitoreo de la seguridad en una base 24x7x365 (24 horas al día, 7 días a la semana, 365 días al año).

El RSII y la Dirección de Tecnologías de la Información deben notificar al Órgano de Gobierno de la SESAJ sobre las debilidades relacionadas con la seguridad de la información, detectadas en la institución.

Respuesta a incidentes de seguridad

Los miembros del ERIS deben estar capacitados para el uso de herramientas adquiridas por SESAJ para el análisis y la respuesta a incidentes de seguridad de la información.

Se deben llevar a cabo reuniones de análisis de los incidentes conforme a la criticidad identificada, para la prevención y su solución.

Los procedimientos de respuesta a incidentes de seguridad deben ser revisados y en caso de ser necesario, actualizados por lo menos anualmente.

El ERISC debe definir dentro de sus procedimientos de Gestión de Incidentes de Seguridad de la Información un proceso de lecciones aprendidas.

Es responsabilidad del ERISC recolectar y documentar la evidencia relativa a los incidentes de seguridad que se identifiquen.

Es responsabilidad de la GESI verificar que se encuentre el resguardo de toda documentación y evidencia de los incidentes relativos a la seguridad de la información dentro de un repositorio para su análisis.

3. Infracciones a la Política de Seguridad de la Información

Las acciones que se enumerar a continuación, de manera enunciativa más no limitativa, constituyen infracciones a la Política de Seguridad de la Información de la SESAJ.

3.1. Acciones de falta u omisión

a) No firmar los acuerdos de confidencialidad o de responsabilidad de activos de información
b) No actualizar la información de los activos de información a su cargo
c) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ellos
d) No guardar de forma segura la información cuando se ausente de su puesto de trabajo o al terminar la jornada laboral
e) Dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, obviando las medidas de seguridad
f) Dejar archiveros o gavetas abiertas, o con las llaves puestas en los escritorios, salvo que se encuentren en el interior de un área que cuente con puerta de acceso, y ésta se encuentre cerrada con llave.
g) Permitir que personas ajenas a la SESAJ deambulen sin acompañamiento en el interior de las instalaciones, en áreas no destinadas a visitas.
h) Solicitar cambio de contraseña de otro usuario
i) No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la SESAJ, para traslado, reasignación o para disposición final (baja).
j) Utilizar claves de acceso de un usuario distinto al propio para ingresar a los sistemas y/o aplicativos

3.2. Acciones de mal uso de la infraestructura tecnológica institucional

a) Hacer uso de la red de datos institucional, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados
b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la infraestructura tecnológica institucional

c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la SESAJ
d) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos de la SESAJ, sin la debida autorización
e) El utilizar la infraestructura tecnológica de la SESAJ para beneficio personal
f) Instalar programas o software no autorizados en las computadoras fijas o portátiles, cuyo uso no esté autorizado por la Dirección de Tecnologías y Plataformas

3.3. Acciones de sabotaje a la infraestructura tecnológica institucional

a) Impedir u obstaculizar el funcionamiento a los aplicativos, bases de datos o a las redes de telecomunicaciones y datos de la SESAJ, sin estar autorizado
b) Destruir, dañar, borrar, deteriorar activos informáticos de la SESAJ, sin autorización
c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la infraestructura tecnológica de la SESAJ
d) Alterar datos personales de las bases de datos institucionales
e) Realizar cambios no autorizados en la infraestructura tecnológica de la SESAJ

3.4. Acciones de acceso no autorizado a la infraestructura tecnológica institucional

a) Acceder sin autorización expresa a todo o parte de los sistemas de la SESAJ
b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos
c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la SESAJ, o permitir que otras personas accedan con el usuario y clave del titular de éstos.
d) Otorgar el acceso o privilegios a la infraestructura de la SESAJ a personas no autorizadas
e) Ingresar a carpetas sin autorización

3.5. Acciones de robo de información a la SESAJ

a) Ejecutar acciones tendientes a eludir o validar los controles de seguridad establecidos por la SESAJ
b) Retirar de las instalaciones de la SESAJ, computadoras fijas, móviles o equipos portátiles que contentan información institucional, sin la autorización pertinente
c) Sustraer de las instalaciones de la SESAJ, documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso
d) Entregar, mostrar y divulgar información institucional a personas o entidades no autorizadas

e) Copiar sin autorización los programas de la SESAJ o violar los derechos de autor o acuerdos de licenciamiento

3.6. Manejo e incumplimiento.

El incumplimiento de las Políticas de la Seguridad de la Información de la SESAJ, dará derecho a ésta a ejercer acciones, procesos y sanciones.

Todos los eventos que tengan relación con la seguridad de la información se comunicarán al Responsable de la Seguridad de la Información.

El Responsable de la Seguridad de la Información, de acuerdo con la gravedad del incidente, informará al Órgano Interno de Control para que en el ámbito de su competencia resuelva lo conducente.

Esta Política, se expide con base en las atribuciones establecidas en el Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco en su artículo 18, fracción III.

Transitorios

ÚNICO. - La presente Política en su versión 1.1, fue aprobada el día 29 del mes de julio del año 2022 por parte de la Secretaría Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco, lo anterior de conformidad con las atribuciones establecidas en el Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco en su artículo 18, fracción III, por lo que entrará en vigor una vez que se le de vista al Órgano de Gobierno, que la Coordinación de Administración las haga de conocimiento de las personas servidoras públicas de la SESAJ y sea publicado en la página web oficial del Organismo.

Hoja de Control de Actualizaciones del Documento

Política General de Seguridad de la Información SESAJ	Versión 1.1

Versión	Fecha	Descripción de las modificaciones
1.0	26/oct/2020	Presentación para conocimiento del Órgano de Gobierno de la SESAJ
1.1	22/jul/2022	• Se incluyó el apartado "Uso de dispositivos tecnológicos personales en la SESAJ" dentro del punto 2.7 Seguridad de los equipos. • Se agregaron algunos conceptos técnicos en las definiciones • Se referenció al "Proceso de respaldo de información, devolución de activos informáticos e inhabilitación de cuentas institucionales" establecido por la Dirección de Tecnologías y Plataformas, dentro del apartado "Terminación o separación del puesto. • Correcciones menores
1.1	18/ago/2022	Presentación para conocimiento del Órgano de Gobierno de la SESAJ, tercera sesión ordinaria.

Dirección de Tecnologías y Plataformas

Secretaría Ejecutiva del Sistema Anticorrupción de Jalisco

Aprobó

Dra. Haimé Figueroa Neri
Secretaria Técnica de la Secretaría Ejecutiva del

Coordinó y supervisó

Dr. Carlos Alberto Franco Reboreda
Director de Tecnologías y Plataformas

Integró

Mtro. Francisco Javier Ulloa Cortez
Subdirector de Proyectos Tecnológicos