PERIÓDICO OFICIAL

DEL GOBIERNO CONSTITUCIONAL DEL ESTADO DE MICHOACÁN DE OCAMPO

Fundado en 1867

Las leyes y demás disposiciones son de observancia obligatoria por el solo hecho de publicarse en este periódico. Registrado como artículo de 2a. clase el 28 de noviembre de 1921.

Directora: Mtra. Fernanda Arizpe Morales

Juan José de Lejarza # 49, Col. Centro, C.P. 58000 **DÉCIMA PRIMERA SECCIÓN** **Tel. 443-312-32-28**

TOMO CXC	Morelia, Mich., Viernes 20 de Marzo de 2026	NÚM. 37

Responsable de la Publicación
Secretaría de Gobierno

DIRECTORIO

Gobernador Constitucional del Estado de Michoacán de Ocampo
Mtro. Alfredo Ramírez Bedolla

Secretario de Gobierno
Lic. Raúl Zepeda Villaseñor

Directora del Periódico Oficial
Mtra. Fernanda Arizpe Morales

Aparece ordinariamente de lunes a viernes.

Tiraje: 40 ejemplares
Esta sección consta de 264 páginas

Precio por ejemplar:
$ 37.00 del día
$ 48.00 atrasado

Para consulta en Internet:
https://periodicooficial.segob.michoacan.gob.mx
www.congresomich.gob.mx

Correo electrónico
periodicooficial@michoacan.gob.mx

CONTENIDO

ANTECEDENTES

1. El 05 de octubre de 2021 se publicó en el Periódico Oficial del Estado de Michoacán, en su séptima sección, la Ley de Gobierno Digital del Estado de Michoacán, en la que, de acuerdo a su artículo primero, uno de sus objetivos es el de establecer los instrumentos mediante los cuales los órganos del Estado implementarán el uso y aprovechamiento estratégico de las tecnologías de la información.
2. El Plan Nacional de Desarrollo Integral del Estado de Michoacán de Ocampo 2021 - 2027, publicado el 08 de agosto de 2022 en el Periódico Oficial del Estado de Michoacán, en su sexta sección, encomienda y confiere facultades a la Secretaría de Finanzas y Administración para hacer realidad el gobierno digital.
3. El 08 de septiembre de 2022 se publicaron en el Periódico Oficial del Estado de Michoacán, en su décima primera sección, los Lineamientos Generales para la Implementación del Gobierno Digital, Uso y Aprovechamiento Estratégico de Tecnologías de la Información y Comunicaciones del Estado de Michoacán.
4. Se publicaron en el Periódico Oficial del Estado de Michoacán, en su décima sección, las Políticas Generales en Materia de Ciberseguridad para las Dependencias y Entidades de la Administración Pública Estatal.

CONSIDERANDO

PRIMERO. El 27 veintisiete de mayo de 2015 dos mil quince, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de combate a la corrupción, entre otros, se modificó el artículo 113, para instituir el Sistema Nacional Anticorrupción, como la instancia de coordinación entre las autoridades de todos los órdenes de gobierno competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de los recursos públicos. Asimismo, se mandató que las entidades federativas establecieran sistemas locales anticorrupción con el objeto de coordinar a las autoridades locales competentes en las materias señaladas; ordenándose en el artículo Séptimo Transitorio la obligación de los sistemas anticorrupción de las entidades federativas de conformarse de acuerdo con leyes generales que resulten aplicables, las constituciones y leyes locales.

SEGUNDO. Al efecto, el 13 trece de noviembre de 2015 dos mil quince, fueron publicadas en el Periódico Oficial del Estado, las reformas a la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo, en materia del combate a la corrupción, adicionando entre otros, el artículo 109 Ter, que establece el Sistema Estatal Anticorrupción como la instancia de coordinación entre las autoridades de todos los órdenes de gobierno de la entidad, competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos.

TERCERO. Por su parte, la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, es un organismo público descentralizado con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión, que tiene como objetivo fungir como órgano de apoyo técnico del Comité Coordinador del Sistema Estatal Anticorrupción, a efecto de proveerle la asistencia necesaria para el desempeño de sus atribuciones. Tiene a su cargo la administración, operación y funcionamiento de los recursos humanos, económicos y materiales que se requieran para el Sistema Estatal Anticorrupción, y cuenta con una estructura operativa para la realización de sus atribuciones, objetivos y fines, tal y como se establece en los artículos 24 y 25 de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo; y 5 Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

CUARTO. Igualmente, al frente de la Secretaría Ejecutiva, hay una persona titular denominada Secretaria Técnica, quien ejerce las funciones de dirección, y se encuentra facultada para elaborar los proyectos de manuales, lineamientos y demás normas que fijen el actuar normativo y organizacional de carácter interno de la Secretaría Ejecutiva y sus modificaciones, así como presentarlos al Órgano de Gobierno para su aprobación. Lo anterior de conformidad con lo dispuesto en los artículos 37 de la Ley del Sistema estatal Anticorrupción de Michoacán; 3, 15, fracción I y 18 fracciones XII, XIII y XIV del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán.

QUINTO. De conformidad con el artículo 5to de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo, los órganos del Estado están obligados a crear y mantener condiciones estructurales y normativas que permitan el adecuado funcionamiento del Estado.

SEXTO. Que en términos del artículo 25 de la Constitución Política de los Estados Unidos Mexicanos, las autoridades de todos los órdenes de gobierno deberán implementar políticas públicas de digitalización de trámites, desarrollo y fortalecimiento de capacidades tecnológicas públicas.

SÉPTIMO. La Ley de Gobierno Digital del Estado de Michoacán establece, en su artículo 5to, la obligación de los órganos del Estado de desarrollar, mantener y actualizar la infraestructura de tecnologías de la información .

OCTAVO. Que los Lineamientos Generales para la Implementación del Gobierno Digital, Uso y Aprovechamiento Estratégico de Tecnologías de la Información y Comunicaciones del Estado de Michoacán, en sus artículos 13, 20, 24, 81, 87, 97 y 98, establece disposiciones que las dependencias y entidades del Estado deberán observar en lo que respecta a ciberseguridad.

NOVENO. Que el presente Manual de Protocolos y Políticas en Materia de Ciberseguridad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, se realizó en observancia de, entre otras leyes y ordenamientos, las Políticas Generales en Materia de Ciberseguridad para las Dependencias y Entidades de la Administración Pública Estatal; y tiene por objeto establecer un marco integral de Ciberhigiene para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, en el cual se considere la evaluación y optimización de prácticas de seguridad informática, así como la protección de los activos de información.

Por lo expuesto y con fundamento en los artículos 30, de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo; 15, fracción I, 16 fracción III,, y 18, fracciones XII y XIII, del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, se emite el siguiente:

ACUERDO

PRIMERO. El Órgano de Gobierno de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, es competente para emitir el presente Acuerdo.

SEGUNDO. Se aprueba la emisión y publicación del Manual de Protocolos y Políticas en Materia de Ciberseguridad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

TERCERO. Se instruye a la Secretaría Técnica para que realice las gestiones necesarias para la publicación de dicho instrumento normativo en la página web de la Secretaría Ejecutiva, así como en el Periódico Oficial del Estado.

Aprobado por unanimidad de votos de las y los ciudadanos, C.P. Marco Antonio Bravo Pantoja, Auditor Superior del Estado de Michoacán; Mtra. Marisol Sánchez Zamudio, Fiscal Especializada en Combate a la Corrupción; Lic. Francisco Ramírez Flores Titular de la Secretaría de Contraloría del Estado; Dra. Laura Elena Alanís García, Magistrada Presidenta Sustituta del Poder Judicial del Estado; Mtra. Azucena Marín Correa, Magistrada de la 5ª Sala del Tribunal en materia Anticorrupción y Administrativa del Estado de Michoacán en representación de la Dra. Lizett Puebla Solórzano, Magistrada Presidenta de dicho Tribunal; L.A. Oscar Chávez Arriaga, Contralor Municipal del Ayuntamiento de Epitacio Huerta; L.C. Rubén Alejandro García Alcántar, Contralor Municipal del Ayuntamiento de Tangamandapio; Lic. María Monserrat Farías Aguirre, Contralora Municipal del Ayuntamiento de Ziracuaretiro; integrantes del Comité Coordinador del Sistema Estatal Anticorrupción, y del Órgano de Gobierno de la Secretaría Ejecutiva del mismo sistema, en la Primera Sesión Ordinaria celebrada el 12 de marzo de 2026 dos mil veintiséis.

Lic. Francisco Ramírez Flores
Presidente del Comité Coordinador y Órgano de Gobierno para efectos de la sesión respectiva.
(Firmado)

Dra. Miryam Georgina Alcalá Casillas
Secretaria Técnica de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, y Secretaria del Comité Coordinador del Sistema Estatal Anticorrupción y del Órgano de Gobierno de la Secretaría Ejecutiva.
(Firmado)

MANUAL DE PROTOCOLOS Y POLÍTICAS EN MATERIA DE CIBERSEGURIDAD DE LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN

CAPÍTULO I
DISPOSICIONES GENERALES

I. Del Objetivo

Establecer un marco integral de Ciberhigiene para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción (SESEA), en el cual se considere la evaluación y optimización de prácticas de seguridad informática, así como la protección de los activos de información.

A través de la aplicación de este marco integral, se pretende lo siguiente:

a) Asegurar la confidencialidad, integridad y disponibilidad de la información institucional;

b) Reducir significativamente los riesgos cibernéticos asociados con la gestión y procesamiento de datos;

c) Garantizar el cumplimiento de las normativas y marcos regulatorios aplicables en materia de Ciberseguridad;

d) Establecer mecanismos de identificación temprana y mitigación de vulnerabilidades en los sistemas informáticos; y,

e) Fomentar una cultura organizacional de Ciberseguridad entre los servidores públicos de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción (SESEA).

II. Del Alcance

El presente Manual de Protocolos y Políticas en materia de Ciberseguridad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción está dirigido a todas las personas servidoras públicas de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción (SESEA) que, en el ejercicio de sus funciones institucionales, interactúan con información y recursos tecnológicos de la organización.

III. **Marco Jurídico**

a) Normativa Internacional de referencia GDPR y normas ISO/IEC 27001 y 27002;

b) Constitución Política de los Estados Unidos Mexicanos, mediante el artículo 6to tercer párrafo y artículo 16 segundo párrafo;

c) Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados;

d) Ley General de Transparencia y Acceso a la Información Pública;

e) Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo;

f) Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo;

g) Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo; y,

h) Políticas Generales en Materia de Ciberseguridad para las Dependencias y Entidades de la Administración Pública Estatal.

IV. **De las Definiciones:**

Para el fin del presente Manual, se entenderá por:

a) Acceso no autorizado**:** A cualquier intento de acceder a un sistema, red o información sin la correspondiente autorización. Este acceso puede ser intencional o accidental y puede comprometer la seguridad de la información;

b) **Activo de información:** A toda la información y/o recurso que tiene valor o es de interés para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, incluyendo documentos, bases de datos y sistemas de información que necesitan protección;

c) **Actualización de Software:** Al proceso de instalar versiones más recientes de software, que a menudo, incluyen correcciones de seguridad para vulnerabilidades descubiertas en versiones anteriores;

d) **Antivirus**: Al software diseñado para detectar, prevenir y eliminar malware de los sistemas informáticos. Su función principal es analizar archivos y programas en busca de comportamientos maliciosos, así como mantener el sistema actualizado con las últimas definiciones de virus;

e) **Aplicación:** Al programa o herramienta informática diseñada para realizar operaciones, tareas o funciones específicas;

f) **Ataque cibernético:** Al intento malicioso de acceder, alterar, destruir o robar información de un sistema o red sin autorización. Esto incluye actividades como el phishing, ransomware, denegación de servicio (DDoS), entre otros;

g) **Autenticación**: Al proceso mediante el cual se verifica la identidad de un usuario, dispositivo o servicio antes de otorgar acceso a sistemas o datos específicos, esto puede incluir el uso de contraseñas, tarjetas de identificación, biometría, entre otros;

h) **Autenticación Multifactor (MFA):** Al método de seguridad que requiere más de un factor para verificar la identidad de un usuario. Los factores típicos son algo que el usuario sabe, tales como la contraseña, algo que el usuario tiene como un teléfono o algo que el usuario es como la huella dactilar o reconocimiento facial;

i) **Backups (copias de seguridad)**: A las copias de los datos y la información almacenada en un sistema, cuyo fin es evitar la pérdida de información en caso de fallos del sistema, ataques de malware o desastres. Las copias de seguridad suelen almacenarse en lugares seguros y ser accesibles para su recuperación;

j) **Borrado Seguro de Discos Duros:** Al procedimiento para asegurar que la información almacenada en discos duros o medios de almacenamiento no pueda ser recuperada después de ser eliminada;

k) **Ciberhigiene**: Al conjunto de prácticas y tecnologías que los usuarios de cualquier sistema, plataforma o herramienta de software que deben aplicar, para garantizar la seguridad y protección de su información digital, así como del hardware, para minimizar los riesgos de ataques y filtraciones de datos;

l) **Ciberseguridad**: A la disciplina que abarca todas las medidas y prácticas implementadas para proteger sistemas, redes y datos de posibles ataques cibernéticos. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información;

m) **Cifrado**: Al proceso de convertir información y datos en un código para prevenir el acceso no autorizado. Solo aquellos que tienen la clave de cifrado pueden descifrar y acceder a los datos originales;

n) **Confidencialidad:** A la propiedad de la información donde se garantiza que solo los individuos autorizados tengan acceso a ella. Es un principio fundamental de la seguridad de la información;

o) **Contraseña**: A la secuencia de caracteres utilizada para autenticar la identidad de un usuario y proporcionar acceso. Esta secuencia debe ser única, compleja y cambiada periódicamente para garantizar la seguridad;

p) **Control de Acceso:** A los mecanismos que regulan quién puede acceder a la información y en qué condiciones. Este mecanismo incluye autenticación (verificación de identidad), y autorización (verificación de permisos) para acceder a la información;

q) **Datos Confidenciales:** A cualquier información que, en caso de ser divulgada sin la debida autorización, podría ocasionar perjuicios a la Secretaría Ejecutiva del Sistema Estatal Anticorrupción o personas servidoras públicas que laboren en dicha Secretaría, comprometer la seguridad de sus partes interesadas o interferir con el cumplimiento efectivo de sus objetivos institucionales;

r) **Datos Electrónicos**: A la información almacenada en formato digital, que incluye documentos, bases de datos, correos electrónicos, entre otros;

s) **Desmagnetización**: Al método de eliminación de datos de medios magnéticos mediante la exposición a un potente campo magnético, el cual descompone la estructura del medio y borra la información;

t) **Destrucción Certificada:** Al servicio provisto por empresas especializadas para eliminar documentos de manera segura, a menudo con una certificación que atestigua que se han destruido correctamente;

u) **Disponibilidad:** A la cualidad de que la información y los recursos estén accesibles y utilizables a solicitud de un usuario autorizado, cuando lo necesite;

v) **Delegación Administrativa:** A la Delegación Administrativa de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

w) **Dirección de Servicios Tecnológicos:** A la Dirección de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

x) **Dirección de Normatividad y Asuntos Jurídicos**: A la Dirección de Normatividad y Asuntos Jurídicos de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

y) **Dirección de Archivos**: A la Dirección de Archivos de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

z) **Equipo auxiliar:** A los dispositivos como máquinas de destrucción de documentos, equipos de climatización, impresoras, escáneres, equipos de respaldo de energía y otros;

aa) **Equipo informático:** Al equipo de cómputo que se utiliza para la realización de tareas relacionadas con las tecnologías de la información, puede ser un monitor, mouse, laptop, router y similares;

bb) **Equipo servidor:** Al equipo de cómputo o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas conocidas como clientes, y que les suministran datos electrónicos;

cc) **Eliminación Segura de Archivos:** Al proceso por el cual se asegura que los datos confidenciales se eliminan, de modo que no puedan ser recuperados ni accedidos nuevamente;

dd) **Firewall (cortafuegos)**: Al dispositivo de seguridad que monitoriza y controla el tráfico de red entrante y saliente, permitiendo o bloqueando datos según un conjunto de reglas de seguridad establecidas. Su objetivo es proteger las redes informáticas de accesos no autorizados y ataques cibernéticos;

ee) **Incidente de seguridad**: Al evento que indica que la seguridad de un sistema o red se ha visto comprometida. Un incidente puede incluir accesos no autorizados, pérdida de información, o cualquier violación de las políticas de seguridad;

ff) **Instalaciones:** Al espacio físico donde se localizan, desenvuelven, y se llevan a cabo reuniones, o trabajo entre personas, así como el espacio donde residen equipos de cómputo, bienes mobiliarios, papelería y demás;

gg) **Información:** A los hechos, eventos, documentos, y/o transacciones de datos relacionados al funcionamiento de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

hh) **Integridad**: A la garantía de que la información es precisa, completa y ha sido protegida contra alteraciones no autorizadas. La integridad asegura que los datos se mantengan en su estado original;

ii) **ISO/IEC 27001:** Information security, cybersecurity and privacy protection - Information security management systems - Requirements. A la Norma implementada para asegurar la estandarización de la seguridad de la información, en la cual se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información. Con esta norma se asegura la confidencialidad e integridad de los datos y la información, así como de los sistemas que la procesan;

jj) **Malware (software malicioso)**: Al programa o conjunto de programas diseñados para infiltrarse en un sistema informático con la finalidad de causar daño, robar información o interrumpir el funcionamiento normal del mismo. Incluye virus, gusanos, troyanos y ransomware;

kk) **Manual**: Al Manual de Protocolos y Políticas en Materia de Ciberseguridad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

ll) **OAuth**: Al protocolo abierto de autorización que permite a las aplicaciones obtener acceso limitado a cuentas de usuario en un servicio HTTP, sin que el usuario comparta sus credenciales;

mm) **Obligación:** Al requerimiento legal o institucional que impone la responsabilidad de proteger información sensible de acuerdo con normas específicas;

nn) **PDE:** A la Plataforma Digital Estatal de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

oo) **Phishing:** A la técnica de fraude en línea que busca engañar a las personas para que proporcionen información confidencial, como nombres de usuario, contraseñas y detalles bancarios, a través de correos electrónicos, mensajes falsos o sitios web fraudulentos;

pp) **Política de Seguridad de la Información:** Al conjunto de reglas y directrices que se establecen para asegurar la protección de sistemas y datos, frente a amenazas internas y externas. Este tipo de políticas por lo general cubren aspectos como el uso de tecnología, acceso a los datos y medidas de seguridad;

qq) **Préstamo**: A la asignación temporal de un activo informático a una persona servidora pública para el cumplimiento de funciones específicas, estableciendo un período determinado de uso y condiciones particulares para su devolución;

rr) **Proveedor de Servicios en la Nube (Cloud Service Provider):** A las empresas que ofrecen servicios de almacenamiento y procesamiento de

datos a través de internet. En estas empresas los datos se gestionan en servidores externos, a menudo en centros de datos ubicados en diferentes partes del mundo;

ss) **Ransomware**: Al tipo de malware que cifra los archivos de un usuario o sistema y solicita un pago (ransom) para restaurar el acceso a dichos archivos. Este tipo de ataque puede ser devastador para las organizaciones;

tt) **Resguardo**: A la responsabilidad asignada a una persona servidora pública para la custodia, cuidado y uso apropiado de un activo informático específico, implicando la obligación de mantenerlo en condiciones óptimas y reportar cualquier incidencia relacionada con su funcionamiento o seguridad;

uu) **Red de comunicación:** Al sistema que conecta dispositivos (computadoras, teléfonos, entre otros.) para permitir el intercambio de información a distancia, generalmente a través de un medio de comunicación compartido como cables o señales inalámbricas;

vv) **Red de Área Local (LAN):** A la red que conecta dispositivos dentro de un área limitada, como una oficina o un edificio. Las LAN permiten compartir recursos como impresoras y archivos;

ww) **Red Privada Virtual (VPN):** A la tecnología que crea una conexión segura y cifrada a través de una red menos segura, como Internet. Una VPN permite a los usuarios enviar y recibir datos de manera segura como si estuvieran conectados a una red privada;

xx) **Sanción**: A la medida disciplinaria como consecuencia de una conducta que infringe una norma jurídica, o por un comportamiento incorrecto;

yy) **Servicio**: A la(s) acción(es) que la Secretaría Ejecutiva del Sistema Estatal Anticorrupción ofrece tanto al exterior como de forma interna a los usuarios que lo necesiten, esto puede ser como; acceso a internet, soporte técnico, correo electrónico, análisis y bloqueo de sitios web no permitidos, mesa de ayuda, entre otros;

zz) **SESEA:** A la Secretaría Ejecutiva del Sistema Estatal Anticorrupción;

aaa) **Sistema de Gestión de Seguridad de la Información (SGSI):** Al conjunto de políticas, procedimientos, marcos normativos y medidas técnicas para gestionar de manera efectiva los riesgos relacionados con la seguridad de la información dentro de una organización;

bbb) **Smishing:** A la técnica de fraude en línea que utiliza mensajes de texto (SMS) falsos, para engañar a las personas y hacer que revelen información confidencial, como contraseñas, datos bancarios o credenciales de acceso, o para inducirlas a hacer clic en enlaces maliciosos que pueden descargar software dañino o redirigir a sitios fraudulentos;

ccc) **Sobrescritura**: A la técnica que implica escribir datos nuevos sobre los datos existentes en un medio de almacenamiento, de forma que los datos originales se vuelven irrecuperables;

ddd) **Soporte de información:** A los dispositivos que permiten almacenar información en formato electrónico, y que en general son fáciles de transportar, por ejemplo: **CD** (Compact Disc), **DVD** (Digital Versatile Disc o Digital Video Disc), **Pendrives** (memorias USB) y similares;

eee) **TI:** A las tecnologías de la información;

fff) **Vida útil**: Al período estimado durante el cual un activo informático puede proporcionar servicios de manera eficiente y económica, considerando factores tecnológicos, funcionales y de obsolescencia;

ggg) **Vishing:** A la técnica de fraude en línea que utiliza llamadas telefónicas fraudulentas para engañar a las personas y hacer que revelen información confidencial, como contraseñas, datos bancarios o detalles personales. Los atacantes suelen hacerse pasar por representantes de instituciones legítimas como bancos o agencias gubernamentales para generar confianza y obtener acceso a datos sensibles; y,

hhh) **Vulnerabilidad:** A la debilidad en un sistema que puede ser explotada por un atacante para causar daño, como errores de software o configuraciones incorrectas en el hardware.

V. **De las Consideraciones:** Todas las políticas en el presente Manual, están sujetas a los puntos siguientes:

a) **Excepciones**

El presente Manual tiene como objetivo establecer un marco integral de Ciberhigiene para la SESEA, orientado a implementar, evaluar y fortalecer prácticas efectivas de seguridad cibernética dentro de la misma SESEA. Su propósito es garantizar la confidencialidad, integridad y disponibilidad de la información institucional, minimizar los riesgos asociados con la gestión de datos, asegurar el cumplimiento normativo, identificar vulnerabilidades en los sistemas tecnológicos, y promover una cultura sólida de Ciberseguridad entre las personas servidoras públicas.

En concordancia con lo anterior, toda política técnica y operativa debe considerar mecanismos para gestionar adecuadamente situaciones excepcionales que, por razones operativas, técnicas, presupuestales o de compatibilidad, requieren apartarse temporalmente de los lineamientos establecidos. Estas situaciones no deben entenderse como una flexibilización de las políticas, sino como casos controlados, justificados y debidamente documentados, donde se autoriza el uso temporal de configuraciones, herramientas o prácticas distintas a las definidas en las políticas institucionales de seguridad tecnológica descritas en el presente Manual.

Estas excepciones solo se concederán cuando exista una justificación sólida, cuenten con las autorizaciones formales requeridas, y estén registradas en los mecanismos oficiales de control tales como las bitácoras o inventarios. Además, deberán establecer un periodo definido de vigencia, medidas compensatorias para mitigar riesgos, y un proceso de revisión periódica para determinar su continuidad, corrección o incorporación como parte de los estándares institucionales.

Cualquier excepción a lo establecido en el presente Manual deberá justificarse mediante un documento formal que incluya una descripción clara de las

condiciones técnicas u operativas que impiden el cumplimiento total de los lineamientos aquí definidos. El documento deberá contener, como mínimo, un análisis de riesgos asociado a la excepción, las medidas compensatorias que se aplicarán y la duración propuesta de la excepción.

Las excepciones serán evaluadas de manera conjunta por la Dirección de Servicios Tecnológicos, la Delegación Administrativa y la Secretaría Técnica de la SESEA, según corresponda al tipo y alcance del activo. Ninguna excepción podrá ser indefinida, y todas deberán contar con una fecha de revisión y renovación o cancelación. Durante la vigencia de la excepción, la Dirección de Servicios Tecnológicos deberá supervisar que las medidas compensatorias se mantengan activas y resulten suficientes para proteger la integridad de la infraestructura tecnológica de la SESEA.

b) Auditorias

La auditoría no solo representa una herramienta de control, sino un componente esencial para fortalecer la gobernanza tecnológica institucional, minimizar riesgos operacionales y regulatorios, y asegurar que las prácticas de Ciberseguridad estén alineadas con los más altos estándares.

En este marco, la Dirección de Servicios Tecnológicos y Plataforma Digital será responsable de diseñar y ejecutar un esquema integral de verificación que abarque auditorías periódicas, registros obligatorios de cambios, monitoreo continuo, métricas de cumplimiento, capacitación técnica especializada y revisiones externas. Este enfoque permitirá evaluar de forma precisa la adherencia a las políticas, identificar posibles brechas, analizar su impacto y establecer planes de remediación con base en evidencia técnica.

En conjunto, este modelo de auditoría no solo permite verificar el cumplimiento normativo, sino que se convierte en un mecanismo de mejora continua que impulsa la eficiencia operativa, refuerza la cultura de Ciberseguridad institucional y protege de forma proactiva la confidencialidad, integridad y disponibilidad de la información pública.

Tomando esto en consideración, la Dirección de Servicios Tecnológicos y Plataforma Digital ejecutará el siguiente protocolo de medidas de seguridad en la SESEA:

1. **Auditorías Periódicas.** Las configuraciones de los activos tecnológicos deben ser auditadas cada seis meses por la Dirección de Servicios Tecnológicos, incluyendo la evaluación automatizada mediante herramientas de escaneo de configuración y revisión manual de controles críticos. Generar reportes detallados con hallazgos, recomendaciones y planes de remediación;

2. **Registro y Trazabilidad.** Toda instalación, configuración o modificación debe quedar registrada en la bitácora técnica institucional o sistema de gestión de activos (Anexo E), incluyendo identificación del responsable, fecha y hora de implementación, descripción detallada del cambio y evidencia de aprobación correspondiente;

3. **Evaluación Continua.** Se debe implementar un proceso de evaluación continua de configuraciones mediante herramientas automatizadas, generando alertas cuando se detecten desviaciones a esta política. Se deben establecer métricas de cumplimiento y reportes gerenciales periódicos;

4. **Capacitación y Concientización.** Se deben desarrollar programas de capacitación continua para personal técnico responsable de implementar y mantener configuraciones seguras, incluyendo actualización sobre nuevas amenazas, mejores prácticas y cambios regulatorios relevantes; y,

5. **Revisión del presente Manual.** El presente Manual será revisado y actualizado de forma anual, o de manera anticipada cuando existan cambios relevantes en el entorno tecnológico, normativo o de riesgo que impacten directamente en las políticas, lineamientos o procedimientos aquí establecidos. Con esta revisión se busca asegurar que las disposiciones contenidas se mantengan alineadas con las mejores prácticas, los estándares de seguridad vigentes y las necesidades operativas de la SESEA.

Las actualizaciones podrán originarse por diversos factores, como la incorporación de nuevas tecnologías, modificaciones en la infraestructura

institucional, cambios en las normativas legales aplicables, recomendaciones derivadas de auditorías internas o externas, evolución en los estándares de Ciberseguridad, o ajustes necesarios tras la detección de vulnerabilidades o incidentes.

La Dirección de Servicios Tecnológicos y Plataforma Digital será responsable de coordinar el proceso de revisión, documentar los cambios efectuados y asegurar que las versiones actualizadas del presente Manual sean comunicadas oportunamente a las áreas responsables de su aplicación. Asimismo, deberá conservar el historial de versiones y mantener disponible la versión vigente para consulta institucional.

Todas las versiones del presente Manual deberán incluir un registro de control de cambios que permita identificar con claridad la fecha de emisión, la versión correspondiente, y un resumen de las modificaciones aplicadas, garantizando así la trazabilidad y transparencia en el proceso de actualización.

VI. **Sanciones por incumplimiento**

El cumplimiento de las políticas, lineamientos, estándares y procedimientos descritos en el presente Manual, es obligatorio para todo el personal que utilice, gestione o administre recursos tecnológicos de la SESEA. Estas disposiciones han sido diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información institucional, así como para garantizar la seguridad operativa y el cumplimiento normativo.

El incumplimiento, negligencia o uso inadecuado de los recursos tecnológicos que derive en la vulneración de estas políticas será considerado un incidente de seguridad institucional. En tales casos, la SESEA podrá aplicar las medidas correctivas, preventivas o disciplinarias correspondientes, como acta administrativa, o en su caso rescisión de contrato y/o realizar la denuncia correspondiente ante las instancias competentes, conforme a lo establecido en su reglamento interno y demás disposiciones administrativas aplicables.

Asimismo, cualquier uso de protocolos, software, configuraciones, dispositivos o prácticas no autorizadas, o la omisión en la notificación de incidentes de seguridad,

será considerado como una infracción a las políticas institucionales de seguridad informática.

La Dirección de Servicios Tecnológicos y Plataforma Digital, en coordinación con la Secretaría Técnica y la Delegación Administrativa, será la responsable de documentar las violaciones detectadas, emitir los reportes técnicos correspondientes, y proponer las acciones disciplinarias o correctivas ante las instancias competentes.

La SESEA se reserva el derecho de realizar auditorías técnicas internas o externas, y en caso de detectar incumplimientos, aplicar las sanciones descritas, con el objetivo de preservar la seguridad del ecosistema digital institucional y fomentar una cultura de responsabilidad tecnológica entre sus servidores públicos.

CAPÍTULO II

DE LA POLÍTICA ACERCA DE LAS RESPONSABILIDADES DE LAS PERSONAS SERVIDORAS PÚBLICAS DE LA SESEA EN PREVENCIÓN DE CIBERATAQUES

I. **Propósito y Objetivo**

Con la implementación de esta política se pretende obtener una gestión eficiente y segura de los equipos y activos informáticos de la SESEA, para que, las personas servidoras públicas que laboran en la SESEA, puedan llevar a cabo sus tareas de la mejor manera posible, sin que sean vulnerables a ningún riesgo informático.

II. **Alcance**

Esta política aplica a todos los activos informáticos que forman parte del patrimonio institucional de la SESEA. Su cobertura incluye equipos de cómputo de escritorio y portátiles, servidores, equipos de comunicación y redes, dispositivos móviles institucionales, impresoras y equipos multifuncionales, así como todo el software y licencias asociadas.

La aplicación de esta política abarca tanto los activos informáticos ubicados en las instalaciones principales de la SESEA, así como aquellos que se encuentran en ubicaciones alternas, sucursales o bajo modalidad de trabajo remoto. Esta política también cubre las responsabilidades asociadas con la seguridad física y lógica de los activos, el cumplimiento de las licencias de Software, y la gestión de incidentes relacionados con estos recursos tecnológicos.

Esta política también alcanza a las personas servidoras públicas que tengan asignados o bajo su resguardo activos o equipos informáticos, estos servidores son los encargados y responsables de mantener la integridad de dichos activos para evitar ataques, y evitar la fuga en información sensible, o aquella que pueda poner en riesgo la integridad de la SESEA.

III. **Responsabilidades**

Las responsabilidades de los principales actores corresponden a:

a) **Secretaría Técnica.** La Secretaría Técnica tiene la responsabilidad de establecer las políticas generales para la gestión de activos informáticos, alineándolas con los objetivos estratégicos institucionales y las mejores prácticas en el sector público. Debe aprobar los lineamientos para la adquisición, asignación y disposición de activos informáticos, asegurando que estos procesos se realicen con base en criterios técnicos, económicos y de transparencia.

Le corresponde autorizar las inversiones significativas en TI, validando que estas contribuyan al cumplimiento de la misión institucional y representen un uso eficiente de los recursos públicos. Asimismo, debe supervisar el cumplimiento de esta política y promover una cultura de responsabilidad y cuidado de los activos informáticos entre todo el personal de la SESEA;

b) **Dirección de Servicios Tecnológicos y Plataforma Digital.** La Dirección de Servicios Tecnológicos y Plataforma Digital es responsable de la implementación técnica de las políticas de gestión de activos informáticos, incluyendo el desarrollo y mantenimiento de inventarios de todos los recursos tecnológicos institucionales. Debe establecer y mantener procedimientos técnicos para la instalación, configuración, mantenimiento y actualización de los activos informáticos. Le corresponde también realizar evaluaciones periódicas del estado y rendimiento de los equipos informáticos, identificando necesidades de actualización, reemplazo o mejora, así como crear un plan para dar mantenimiento preventivo y correctivo a los equipos de cómputo. Debe proporcionar soporte técnico especializado a los usuarios finales y coordinar con proveedores cuando sea necesario. Asimismo, debe implementar y supervisar las medidas de seguridad informática necesarias para proteger los activos tecnológicos institucionales;

c) **Delegación Administrativa.** La Delegación Administrativa tiene la responsabilidad de gestionar los aspectos administrativos y patrimoniales de los activos informáticos, incluyendo su registro en el inventario institucional, la tramitación de procesos de adquisición, y el control de la documentación relacionada con garantías, contratos de mantenimiento y seguros. Le corresponde también coordinar los procesos de asignación y reasignación de activos informáticos, asegurando que se cumplan los procedimientos establecidos y se mantenga la documentación actualizada. Debe supervisar el cumplimiento de las obligaciones contractuales relacionadas, y gestionar los

procesos de baja y disposición final de equipos obsoletos o fuera de servicio; y,

d) **Personas Servidoras Públicas de la SESEA.** Las personas servidoras públicas de la SESEA, personal de estructura, personal por honorarios y/o usuarios finales, que tienen bajo resguardo o préstamo algún bien informático, son responsables del cuidado de dicho equipo, uso apropiado y conservación en sus condiciones óptimas. Deben utilizar los activos informáticos exclusivamente para fines institucionales y de acuerdo con las políticas de uso establecidas por la SESEA. También tienen la obligación de reportar inmediatamente cualquier daño, mal funcionamiento, pérdida o robo de los activos informáticos bajo su responsabilidad. Deben permitir y facilitar las actividades de mantenimiento, actualización e inspección de los equipos cuando sea requerido por la Dirección de Servicios Tecnológicos y Plataforma Digital. Asimismo, deben devolver los activos informáticos en las condiciones en que les fueron entregados al finalizar su encargo o cuando sean requeridos por la SESEA.

IV. Procedimientos de Asignación y Control

La asignación de activos informáticos debe realizarse mediante un proceso formal que incluya la identificación clara del activo, la persona responsable, las condiciones de uso y el período de asignación. Se debe generar un documento donde se detalle el estado del activo y las responsabilidades asociadas.

El control y seguimiento de los activos asignados debe realizarse mediante un sistema de información que permita el monitoreo continuo de su ubicación, estado y uso. Se deben realizar verificaciones físicas periódicas para confirmar la existencia y condiciones de los activos, identificando cualquier discrepancia que requiera atención inmediata.

V. Seguridad de la información

Todos los activos informáticos deben contar con medidas de seguridad física y de Software apropiadas para su naturaleza y valor. Los usuarios finales deben implementar controles de acceso adecuados, mantener actualizadas las medidas de protección contra Malware, y asegurar que la información contenida en los activos esté debidamente respaldada.

VI. **Gestión de Incidentes y No Conformidades**

En caso de incidentes relacionados con los activos informáticos de la SESEA, se debe notificar a la Dirección de Servicios Tecnológicos, documentando detalladamente la situación. Posteriormente, se debe realizar una investigación para determinar las causas del incidente y establecer medidas correctivas y preventivas.

CAPÍTULO III
DE LA POLÍTICA PARA LA VALIDACIÓN DE SOFTWARE

CIS CONTROL #2: INVENTARIO Y CONTROL DE ACTIVOS DE SOFTWARE

I. Propósito y Objetivo

En esta política se busca asegurar la integridad, seguridad y funcionalidad óptima del entorno tecnológico de la SESEA, mediante el uso de aplicaciones que cumplan con estándares de calidad, reciban actualizaciones de seguridad periódicas y mantengan compatibilidad con los sistemas institucionales. Asimismo, con esto se pretende establecer procedimientos claros para la identificación y sustitución de Software obsoleto, con el fin de minimizar los riesgos cibernéticos y garantizar el cumplimiento de las obligaciones legales en materia de propiedad intelectual y licenciamiento de Software.

II. Alcance

Esta política se aplica de manera general a todos los dispositivos tecnológicos, sistemas informáticos y Software utilizados dentro de la SESEA. Su cobertura abarca computadoras de escritorio, laptops, servidores, equipos móviles institucionales, tablets, y cualquier dispositivo que forme parte del entorno tecnológico de la secretaría.

La política incluye todo el Software instalado o utilizado en estos dispositivos, desde sistemas operativos hasta aplicaciones especializadas, herramientas de productividad, Software de seguridad, navegadores web, aplicaciones de comunicación y sistemas internos desarrollados específicamente para la SESEA. También comprende las plataformas web institucionales, bases de datos, y cualquier aplicación que interactúe con los sistemas de la Plataforma Digital Estatal.

El alcance se extiende a todo el personal que utilice equipos tecnológicos institucionales, incluyendo personas servidoras públicas de todas las unidades responsables.

Asimismo, incluye las responsabilidades de proveedores de Software, servicios de TI, y cualquier tercero que proporcione soporte técnico o mantenimiento a los sistemas institucionales.

III. **Descripción de la política**

Todos los dispositivos tecnológicos utilizados en la SESEA, incluyendo computadoras, laptops, servidores, equipos móviles y sistemas informáticos, deben operar exclusivamente con Software que cuente con soporte oficial por fabricante o proveedor. Esto significa que el único Software permitido es aquel que cuenta con las condiciones siguientes:

a) **Recibe actualizaciones de seguridad.** El Software autorizado debe recibir parches periódicos emitidos por el fabricante para corregir errores y vulnerabilidades detectadas. Estas actualizaciones se aplican automáticamente o bajo control técnico especializado, con el propósito de prevenir ataques cibernéticos, infecciones de Malware o accesos no autorizados que puedan comprometer la integridad de los sistemas institucionales;

b) **Está dentro de su ciclo de vida oficial.** Todo Software tiene un período determinado durante el cual el fabricante garantiza su funcionamiento, compatibilidad y soporte técnico, conocido como ciclo de vida de soporte. Una vez finalizado este ciclo, el Software se considera obsoleto, incluso si continúa operando aparentemente sin problemas. Se prohíbe el uso de Software fuera de su ciclo de vida debido a que pueden surgir riesgos técnicos significativos y problemas legales, como el incumplimiento de normativas de protección de datos o estándares de calidad institucional;

c) **Es compatible con otros sistemas institucionales.** El Software compatible asegura la funcionalidad e interoperabilidad con los demás componentes del entorno tecnológico, incluyendo sistemas operativos, redes, bases de datos y plataformas web institucionales. Esta compatibilidad evita que las aplicaciones causen errores, conflictos o pérdida de datos al interactuar con otros sistemas, mejorando simultáneamente el rendimiento general del ecosistema tecnológico y reduciendo significativamente el número de incidencias técnicas; y,

d) **Cuenta con soporte técnico activo.** El Software debe mantener disponibilidad de asistencia técnica oficial por parte del fabricante o proveedor autorizado, garantizando acceso a documentación actualizada, resolución de incidentes y orientación especializada. Esta condición permite que la Dirección de Servicios Tecnológicos y Plataforma Digital, pueda resolver problemas técnicos de manera eficiente, acceder a parches de seguridad oportunos y recibir asesoría directa para optimizar el funcionamiento del Software dentro del entorno institucional, con el fin de dar continuidad operativa y minimizar tiempos de inactividad.

Derivado de estos criterios de seguridad, compatibilidad y soporte técnico, a continuación, se presenta una lista del Software que la Dirección de Servicios Tecnológicos ha detectado que cumplen con dichos requerimientos.

Categoría	Software Permitido (Soportado)	Software No Permitido (Obsoleto o No Soportado)	Observaciones
Sistemas Operativos	Windows 11 Pro / Enterprise Ubuntu 22.04 LTSmacOS 13+ (Ventura o superior)	Windows inferior a ver 8.1, Ubuntu inferior a ver 16.04, y macOS inferior a ver 10.13	Versiones inferiores al software descrito dejaron de recibir soporte
Ofimática	Microsoft Office 365 (en la nube) Microsoft Office 2019 LibreOffice 7.x	Microsoft Office 2010 Office 2013 sin parches, LibreOffice 5.x	Office 2010 o versiones anteriores, dejaron de recibir soporte en 2020
Antivirus y Seguridad	Microsoft Defender actualizado McAfee, ESET o Sophos.	Versiones antiguas sin firma actualizada Antivirus gratuitos sin soporte	Los antivirus sin actualizaciones no detectan amenazas actuales.
Navegadores Web	Microsoft Edge (última versión) Google Chrome actualizado Mozilla Firefox ESR	Internet Explorer 11 Chrome v88 o anterior Netscape / Safari antiguos	Internet Explorer fue retirado oficialmente por Microsoft. No debe usarse.
Herramientas de Comunicación	Microsoft Teams Zoom actualizado Google Meet vía navegador seguro	Skype clásico sin actualizaciones MSN Messenger Zoom v5.0 o inferior	Las versiones viejas de Zoom tienen vulnerabilidades graves, no parcheadas.
Software Especializado	Adobe Acrobat DCSPSS versión vigente con soporte	Autocad 2012 Adobe CS6 (sin Creative Cloud) SPSS v19 o inferior	Las versiones antiguas pueden no ser compatibles con sistemas actuales.
Sistemas Internos	ERP institucional versión actualizada Plataformas web internas en mantenimiento activo	Versiones no actualizadas, con módulos sin mantenimiento	Se deben planificar migraciones si el sistema interno ha quedado sin soporte.

IV. **Responsabilidades**

La Secretaría Técnica tiene la responsabilidad de revisar y aprobar en caso de ser necesario, los criterios de inclusión y exclusión de contactos a la lista de Software.

La Dirección de Servicios Tecnológicos tiene la responsabilidad principal de mantener la lista actualizada de Software y compartirla con las personas servidoras públicas que laboran en la SESEA. Esta actualización debe realizarse al menos una vez cada seis meses, o cuando se anuncien terminaciones de soporte por parte de los fabricantes. Esta periodicidad asegura que la SESEA mantenga un inventario actualizado de herramientas tecnológicas aprobadas y elimine aquellas que representen riesgos de seguridad. La Dirección de Servicios Tecnológicos también debe asegurar que todos los cambios sean documentados y comunicados a las unidades correspondientes.

La Dirección de Servicios Tecnológicos también es la unidad responsable final de la evaluación y aprobación de todas las solicitudes relacionadas con Software institucional, garantizando así que las decisiones se alineen con los objetivos estratégicos y de seguridad de la SESEA.

La Dirección de Normatividad y Asuntos Jurídicos junto con la Delegación Administrativa son los responsables de validar los contactos externos, especialmente aquellos relacionados con las autoridades competentes. Deben verificar que estos contactos cumplan con los requisitos legales y contractuales aplicables, esto en el supuesto de adquirir nuevo Software o servicios.

Finalmente, las personas titulares de cada Unidad Responsable, tienen la responsabilidad de revisar periódicamente los activos digitales que se encuentren a su resguardo y solicitar a la Secretaría Técnica y la Dirección de Servicios Tecnológicos, si es necesario, la adscripción de nuevos activos tecnológicos, siempre y cuando, dichos activos le permitan realizar de una mejor manera las actividades que realizan en la SESEA. Esto con respecto a la “Guía de procedimientos para la Revisión y Gestión de Software Institucional”.

V. **Normativas de referencia**

Esta política se basa en las mejores prácticas internacionales establecidas por los CIS Controls v8, específicamente el Control 17.1 relacionado con la gestión de incidentes. También se alinea con los estándares ISO/IEC 27035 para la gestión de

incidentes de seguridad de la información y sigue las directrices del NIST SP 800-61 Computer Security Incident Handling Guide.

VI. Guía de procedimientos para la Revisión y Gestión de Software Institucional

a) Política de Autorización de Software

Todo Software que no esté incluido en la relación oficial de aplicaciones requiere autorización previa y una evaluación técnica exhaustiva antes de su implementación en el entorno tecnológico institucional. Esta medida preventiva busca garantizar la seguridad, compatibilidad y eficiencia operativa de todos los sistemas que integran la Plataforma Digital Estatal.

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de validar cualquier Software antes de permitir su uso institucional, analizando el impacto que tendrá en la organización. Esta evaluación integral considera aspectos de seguridad, compatibilidad técnica, recursos necesarios y alineación con los objetivos institucionales, con el fin de evitar infiltraciones maliciosas, daños o perjuicios a los sistemas críticos. Las solicitudes de nuevo Software deben realizarse mediante el documento especificado en el Anexo A.

b) Procedimientos para reconocer Software Obsoleto

El Software obsoleto se define como cualquier programa o sistema que ya no recibe soporte del proveedor, carece de actualizaciones de seguridad, o ha sido reemplazado oficialmente por versiones más recientes. La gestión adecuada de Software obsoleto es fundamental para mantener la integridad y seguridad de los sistemas institucionales. Por ello, la Dirección de Servicios Tecnológicos realiza los pasos siguientes:

1. **Identificación y reporte.** El Software obsoleto puede detectarse mediante diferentes mecanismos como lo es el mantenimiento programado, el cual representa el método más eficiente, donde la Dirección de Servicios Tecnológicos realiza revisiones técnicas. Adicionalmente, cualquier usuario puede reportar cuando una aplicación presenta mal funcionamiento, muestra advertencias

persistentes o no se actualiza correctamente, lo cual puede indicar obsolescencia;

2. **Validación técnica.** Una vez identificado el Software potencialmente obsoleto, el personal técnico de la Dirección de Servicios Tecnológicos y Plataforma Digital procede a verificar su estado actual. El proceso de validación determina si el Software ya no recibe actualizaciones de seguridad críticas, si está fuera del ciclo de vida oficial establecido por el fabricante, o si ha sido declarado obsoleto y reemplazado por otra versión. También se verifica si existe alguna excepción previamente aprobada por necesidades específicas o consideraciones temporales que justifiquen su uso continuado;

3. **Análisis de impacto.** Antes de proceder con cualquier acción correctiva, se realiza un análisis integral del impacto que podría generar la eliminación del Software obsoleto. Este análisis incluye una revisión exhaustiva de dependencias, verificando si el Software está vinculado a procesos internos críticos, flujos de trabajo establecidos, equipos periféricos específicos, o integrado con otros sistemas institucionales.

   La consulta con usuarios responsables y áreas funcionales es fundamental para determinar si la aplicación es crítica para las operaciones diarias o si puede ser reemplazada sin afectar la productividad. Simultáneamente, se realiza una evaluación de riesgo que prioriza la búsqueda de soluciones seguras cuando el Software obsoleto sigue siendo utilizado en operaciones clave, evitando interrupciones operativas;

4. **Implementación de soluciones.** Una vez completado el análisis de impacto, se implementan las medidas correctivas más apropiadas según cada situación específica. La actualización representa la primera opción, instalando la versión más reciente del mismo Software cuando está disponible y ha sido previamente aprobada por la Dirección de Servicios Tecnológicos.

Cuando no existe una versión reciente o compatible, se procede al reemplazo del Software obsoleto con una alternativa funcional equivalente, previa validación de la Dirección de Servicios Tecnológicos, Delegación Administrativa y la Secretaría Técnica según corresponda. En casos excepcionales donde no hay alternativas viables, se analiza una modificación en el proceso de trabajo, coordinando estrechamente con el área afectada para minimizar el impacto operativo;

5. **Eliminación segura.** El personal técnico de la Dirección de Servicios Tecnológicos ejecuta la desinstalación del Software obsoleto siguiendo protocolos seguros y controlados. Este proceso utiliza Software especializado externo o herramientas incluidas dentro del sistema operativo para eliminar completamente el programa y todas sus extensiones relacionadas.

   La eliminación incluye la revisión y limpieza de carpetas residuales, servicios que puedan quedar ejecutándose en segundo plano, y archivos de configuración que podrían permanecer activos tras la desinstalación estándar. Finalmente, se verifica que el dispositivo funcione correctamente después de la eliminación y que no existan conflictos con otros programas instalados; y,

6. **Documentación y seguimiento.** Toda acción realizada debe quedar debidamente registrada para asegurar trazabilidad y control administrativo. Se genera o actualiza la bitácora de Software no soportado especificada en el Anexo B, documentando el nombre del Software eliminado, usuario y equipo afectado, fecha y hora de la intervención, y el responsable técnico de la acción.

   La comunicación con el usuario incluye información detallada sobre la acción realizada, el nuevo Software instalado cuando se aplique, y recomendaciones específicas de uso y mantenimiento para prevenir futuros inconvenientes.

c) Consideraciones Especiales

La instalación de Software obsoleto está estrictamente prohibida sin la aprobación expresa de la Dirección de Servicios Tecnológicos. Esta medida preventiva evita la introducción de vulnerabilidades conocidas y mantiene la integridad del ecosistema tecnológico institucional.

En situaciones excepcionales donde se requiera una excepción temporal, debe solicitarse formalmente mediante oficio dirigido a la Dirección de Servicios Tecnológicos y Plataforma Digital y/o Secretaria Técnica. Esta solicitud debe acompañarse del documento citado en el Anexo A y registrarse obligatoriamente en la Bitácora del Anexo B para mantener un control adecuado.

Se recomienda a todos los usuarios mantener sus aplicaciones actualizadas y reportar inmediatamente cualquier error, alerta del sistema o comportamiento anómalo a la Dirección de Servicios Tecnológicos. Esta colaboración activa fortalece la seguridad general y permite una respuesta rápida ante posibles amenazas.

d) Información de Contacto

Para consultas técnicas, solicitudes de actualización o reportes de incidentes relacionados con Software, los usuarios pueden contactar al área técnica a través del correo plataformadigital@seseamichoacan.mx o mediante las extensiones telefónicas 1013, 1001, y 1023.

CAPÍTULO IV
DE LA POLÍTICA PARA ELIMINAR EL SOFTWARE NO AUTORIZADO

CIS CONTROL #2: INVENTARIO Y CONTROL DE ACTIVOS DE SOFTWARE

I. Propósito y Objetivo

Establecer un mecanismo de control riguroso y documentado sobre el uso de Software en todos los activos tecnológicos de la SESEA, con el fin de garantizar que únicamente se utilice Software previamente autorizado por la Dirección de Servicios Tecnológicos y Plataforma Digital, Delegación Administrativa y Secretaria Técnica. Esta tercera política tiene como finalidad principal:

a) Asegurar el cumplimiento de las políticas institucionales en materia de Ciberseguridad y licenciamiento;

b) Revisar regularmente qué programas están instalados en las computadoras, identificar aquellos que no están autorizados y llevar un registro claro de ellos;

c) Documentar y dar seguimiento a los casos especiales en los que se ha permitido el uso de programas fuera de la lista oficial autorizada, siempre y cuando tengan una justificación válida y estén aprobados formalmente; y,

d) Así como establecer una calendarización de revisiones periódicas en cada una de las áreas que conforman a la SESEA, con el propósito de mantener un entorno tecnológico seguro, actualizado y conforme con las mejores prácticas de Ciberhigiene institucional.

II. Alcance

Esta política aplica a todos los activos tecnológicos como lo son las computadoras, servidores, dispositivos móviles, Software y servicios digitales utilizados dentro de la SESEA, así como al personal que los opera. Su implementación abarca el control, registro y supervisión del Software instalado en dichos activos, clasificándolos en tres categorías: autorizado, no autorizado y excepciones

documentadas. Se incluyen actividades como la revisión periódica de equipos, la detección y eliminación controlada del Software no autorizado, la documentación y seguimiento de excepciones justificadas, y la adopción de medidas preventivas para evitar futuras infracciones. Todo lo anterior contribuye a mantener un entorno tecnológico seguro, actualizado, eficiente y conforme con las mejores prácticas de Ciberhigiene y las políticas de seguridad de la información vigentes en la SESEA.

III. **Descripción de la política**

Con el objetivo de mantener un entorno tecnológico seguro, eficiente y conforme con las políticas de seguridad de la información de la SESEA, el Software se clasifica en tres categorías principales:

a) Software Autorizado. Incluye todo aquel Software que ha sido debidamente aprobado por la Dirección de Servicios Tecnológicos y Plataforma Digital, la Delegación Administrativa y la Secretaría Técnica, para su instalación y uso en los activos tecnológicos de la SESEA. Este Software cumple con los lineamientos establecidos en materia de seguridad informática, licenciamiento legal y funcionalidad operativa. Su instalación, configuración y actualización se realiza de manera controlada, a través de herramientas de gestión centralizada o por personal autorizado del área de la Dirección de Servicios Tecnológicos y Plataforma Digital, garantizando su correcta implementación y mantenimiento. Ejemplos: Navegadores aprobados, antivirus corporativos, herramientas de comunicación oficial, entre otros.

Tabla de Software autorizado dentro de la SESEA.

Nombre del Software	Versión	Uso Aprobado	Departamento Responsable	Observaciones
Microsoft Office 365	Última	Productividad	DSTPD / General	Licencia corporativa activa
Microsoft Project Plan3	Última	Productividad	DSTPD / ST	Licencia corporativa activa
Workspace Business Standard	Última	Gestión de correos institucionales	DSTPD / General	Licencia corporativa activa
Canva Pro	Última	Productividad	DSTPD / ST	Licencias verificadas
Adobe Creative Cloud	Última	Productividad	DRPPEV / UVCI	Licencias verificadas

Google Chrome	Última	Navegación	DSTPD / General	Actualizaciones automáticas habilitadas
Firefox	Última	Navegación	DSTPD / General	Actualizaciones automáticas habilitadas
Facebook	Última	Transmisiones en vivo	DSTPD / UVCI	
YouTube	Última	Transmisiones en vivo	DSTPD / UVCI	
Zoom	Última	Videollamadas	Recursos Humanos / General	Autenticación SSO activa
Aspel Noi	Última	Gestión de nómina y administración de personal	DA	Licencias verificadas
Licencia Aspel Facture	Última	Facturación electrónica y emisión de CFDI	DA	Licencias verificadas
Certificado SSL Multidominio	Última	Protección de sitios web institucionales mediante cifrado HTTPS	DSTPD	Certificado SSL de tipo multidominio que permite asegurar hasta 3 dominios/subdominios institucionales
Google One	Última	Almacenamiento en la nube, respaldo y sincronización de archivos institucionales	DSTPD/ General	Licencias verificadas
Business Web Hosting	Última	Hospedaje de sitios institucionales, bases de datos y servicios web	DSTPD	Licencias verificadas
Extension Joomla	Actualizadas	Página web SESEA	DSTPD	Licencia activa
Dominio institucional: seseamichoacan.com	Última	Portal web oficial de la SESEA	DSTPD	Licencia activa
Licencia KVM (Virtualización basada en Linux)	Última	Plataforma de virtualización para servidores o entornos de desarrollo	DSTPD	Licencia activa
Licencia Labs Mobile	Última	Envío de notificaciones institucionales por SMS	DSTPD	Licencia activa

Replika (software de respaldo)	Última	Respaldo y recuperación de datos en servidores o sistemas institucionales	DSTPD

La presente lista contiene el Software actualmente autorizado para instalación y uso en los activos tecnológicos de la SESEA. No obstante, esta relación no debe interpretarse como limitativa o definitiva. En caso de requerir el uso de un Software que no se encuentre listado, el área solicitante puede solicitarlo a través del inciso c) Excepciones Documentadas.

b) Software No Autorizado. Este tipo de Software representa un riesgo significativo para la integridad, disponibilidad y confidencialidad de los activos tecnológicos de la SESEA, ya que puede:

1. Introducir vulnerabilidades o Malware;

2. Generar conflictos con Software crítico o con configuraciones de red y seguridad;

3. Requerir permisos elevados sin supervisión técnica;

4. Incumplir con licencias comerciales o con la Ley de Protección de Datos Personales; y,

5. Desviar el uso de recursos institucionales para fines no relacionados con la función pública.

Se entiende por Software no autorizado todo aquel programa, aplicación, complemento, extensión o herramienta digital que:

1. No ha sido aprobado formalmente por la Dirección de Servicios Tecnológicos y Plataforma Digital;

2. No cuenta con un dictamen técnico favorable en cuanto a seguridad, funcionalidad o licenciamiento;

3. Ha sido instalado sin solicitud previa ni autorización; y,

4. Se considera innecesario, duplicado o incompatible con los sistemas, procesos o lineamientos institucionales.

Por lo tanto, su uso está estrictamente **prohibido** en los equipos, servidores, redes, o dispositivos bajo control de la SESEA.

Lista de Software no Autorizado.

Nombre del Software	Versión	Categoría	Motivo de No Autorización
uTorrent / BitTorrent	N/A	Compartición de archivos (P2P)	Riesgo de seguridad / P2P no permitido
CCleaner	N/A	Optimización del sistema	Potencial de conflicto con software corporativo
TeamViewer (sin licencia institucional)	N/A	Acceso remoto	Control remoto sin trazabilidad ni autorización. Uso personal frecuente.
Reproductores multimedia tipo VLC con complementos	N/A	Multimedia	Algunos complementos permiten la ejecución de scripts o codecs no seguros. Requiere control.
Navegadores no corporativos (Brave, Opera GX)	N/A	Navegadores	Pueden tener VPNs o extensiones activas por defecto. No permiten control administrativo.
Juegos instalados localmente (ej. FreeCell, Solitario, Steam)	N/A	Ocio / No laboral	No tienen justificación funcional. Uso inadecuado de recursos públicos.

c) Excepciones Documentadas. Este apartado corresponde a Software que, si bien no cumple completamente con los criterios establecidos en las políticas generales de uso de Software institucional, ha sido aprobado de manera excepcional por la Secretaría Técnica, Delegación Administrativa y la Dirección de Servicios Tecnológicos y Plataforma Digital debido a una necesidad justificada y es de uso temporal.

Las excepciones son evaluadas y se otorgan únicamente cuando:

1. Existe una justificación técnica o funcional sólida por parte del área solicitante;

2. No hay una alternativa autorizada que cumpla con los mismos requerimientos;

3. El uso del Software no compromete la seguridad, estabilidad ni integridad de los activos institucionales; y,

4. Se acepta bajo condiciones controladas, como su uso en entornos aislados, restricciones de red, supervisión técnica, o limitación por tiempo o tarea.

Cada Software requerido debe ser solicitado, sin excepción, a través de un oficio y el formato de autorización (Anexo A) debidamente firmado por la:

1. Secretaría Técnica;

2. Delegación Administrativa; y,

3. Dirección de Servicios Tecnológicos y Plataforma Digital.

Esto deberá quedar debidamente registrado en el inventario de excepciones, el cual será administrado por la Dirección de Servicios Tecnológicos y Plataforma Digital conforme a lo establecido en el Anexo B, y deberá ser revisado periódicamente (**al menos una vez al mes**) para evaluar si la excepción sigue siendo válida, si puede eliminarse o si debe considerarse su incorporación como Software autorizado.

El Software que se considera como excepción dado su aplicación dentro de las instalaciones de la SESEA corresponde a la tabla siguiente:

Nombre del Software	Justificación	Aprobado Por	Acción
VirtualBox	Pruebas de entornos virtuales de desarrollo	DSTPD	Bloqueado. Solo se permite uso por DSTPD.
FileZilla	Permite acceso FTP sin control centralizado; riesgo de filtración	DSTPD	Bloqueado. Solo se permite uso por DSTPD con excepción documentada (SFTP únicamente)
AnyDesk	Necesario para acceso remoto en Mesa de Ayuda	DSTPD	Bloqueado. Solo se permite uso por DSTPD
Aplicaciones de redes sociales (Facebook, TikTok, Instagram)	Necesario para llevar las redes sociales de la SESEA	ST	Solo se permite uso por la DSTPD Y UVCI

Nota final, el empleo de Software fuera de los términos establecidos o sin autorización vigente será considerado una violación a las políticas de seguridad informática de la SESEA.

Para mantener la seguridad, integridad y buen funcionamiento de los sistemas institucionales, es fundamental asegurar que todo el Software instalado cumpla con las políticas y normativas establecidas por la SESEA. El uso de Software no autorizado puede generar riesgos de seguridad, problemas legales y afectar el desempeño de los equipos. Es por esto que a continuación se presentan las reglas básicas para identificar software no autorizado, así como la eliminación del mismo, con el fin de garantizar un control adecuado y proteger los recursos tecnológicos de la SESEA.

IV. **Reglas básicas para identificar Software no autorizado**

a) **No tener una licencia válida o institucional**

Se considera Software no autorizado aquel que no tenga una licencia legal o institucional válida, como el Software pirateado o “crackeado”, que no forme parte de las licencias oficiales adquiridas por la SESEA o que no cuente con documentos o contratos que justifiquen su uso legal; por ejemplo, usar Microsoft Office con una clave no adquirida por la organización. Además, todo Software debe ser revisado y aprobado formalmente por el área de tecnología antes de ser utilizado.

b) **No estar aprobado formalmente por la Dirección de Servicios Tecnológicos y Plataforma Digital**

El Software debe ser evaluado y aprobado por el departamento o área responsable de tecnología, en este caso la Dirección de Servicios.

Ejemplo: Instalar una herramienta de gestión de tareas sin consultar al área de TI, aunque sea útil para el trabajo.

c) **Tener funciones que puedan poner en riesgo la seguridad o privacidad**

Se considera no autorizado cualquier Software que, por su funcionamiento, represente un riesgo para la seguridad, la privacidad o el control institucional. Esto incluye programas que recolectan información sensible sin el conocimiento o consentimiento del usuario, aquellos que impiden o dificultan el seguimiento de actividades dentro de los sistemas institucionales lo que afecta la trazabilidad y la rendición de cuentas, así como aquellos que pueden introducir Malware, virus u otros elementos que comprometan la integridad de los equipos o permitan accesos no autorizados a la red institucional.

Ejemplos comunes de este tipo de Software son las aplicaciones de control remoto no aprobadas, VPNs personales que ocultan el tráfico de red, o navegadores modificados que bloquean los sistemas de monitoreo o registro implementados por el área de la Dirección de Servicios Tecnológicos.

d) **Ser para uso personal, entretenimiento o no relacionado con el trabajo**

Se considera Software ajeno a las funciones públicas todo aquel programa o aplicación que esté destinado al uso personal, al entretenimiento o a actividades que no guardan relación directa con las tareas y responsabilidades institucionales. Aunque este tipo de Software pueda ser legal y no represente un riesgo técnico evidente, su uso dentro del entorno laboral no está justificado y, por lo tanto, se considera no autorizado. Esto incluye juegos instalados en los equipos, plataformas de

streaming de música o video, editores de contenido personal y redes sociales que no estén vinculadas a funciones oficiales o institucionales.

e) **Estar diseñado para eludir controles de red, políticas o bloqueos institucionales**

Se considera Software inseguro cualquier programa que esté diseñado para evitar o evadir las restricciones de seguridad establecidas por la Dirección de Servicios Tecnológicos y Plataforma Digital. Esto incluye aplicaciones que interfieren con los controles implementados para proteger los sistemas, como el uso de proxies, VPNs personales, herramientas de anonimato o navegadores modificados que dificultan la supervisión del uso de los equipos. Estos programas representan un riesgo porque pueden abrir puertas a accesos no autorizados, permitir la conexión a sitios bloqueados o impedir el monitoreo necesario para mantener la integridad y seguridad de la red institucional.

V. Reglas para la Eliminación del Software No Autorizado

Para asegurar una eliminación segura, formal y conforme con las políticas de la SESEA, se establecen los siguientes pasos una vez identificado el Software no autorizado en los dispositivos institucionales:

a) **Revisión técnica y validación del caso**

El personal de la Dirección de Servicios Tecnológicos debe confirmar que el Software detectado efectivamente no cumple con los lineamientos establecidos. Para ello, se realizará una revisión con base en las *Reglas básicas para identificar Software no autorizado*, evaluando su origen, propósito y posible impacto en el funcionamiento del sistema. En caso de que el Software cuente con una excepción previamente aprobada, ésta deberá estar debidamente documentada. Si no existe justificación válida para su uso, se procederá con su eliminación.

b) **Notificación al usuario responsable**

Una vez validado el hallazgo, se notificará al usuario responsable del equipo donde se detectó. Esta notificación debe ser clara y oportuna, con el objetivo de que el usuario entienda la situación y las razones por las cuales el Software será eliminado. En ella se debe explicar brevemente por qué el programa no cumple con las políticas de la organización, lo cual puede deberse a que no cuenta con una licencia válida, no fue aprobado o representa riesgos para la seguridad institucional.

c) **Desinstalación controlada**

Una vez confirmada la presencia de Software no autorizado y determinada la necesidad de eliminarlo, el proceso de desinstalación debe realizarse de manera planificada, segura y sin afectar la operatividad del equipo. Para ello, se deberán utilizar herramientas oficiales de administración de Software que permitan gestionar el ciclo de vida de las aplicaciones, como plataformas de distribución centralizada o sistemas de gestión de activos tecnológicos. Estas herramientas garantizan que la eliminación sea completa, incluyendo archivos asociados, configuraciones residuales y entradas en el registro del sistema.

Si por alguna razón es necesario realizar la eliminación de forma manual, el personal técnico deberá proceder con suma precaución, revisando que no se modifiquen configuraciones importantes del sistema ni se borren archivos esenciales para el funcionamiento de otras aplicaciones. En todo momento se debe asegurar que el proceso no interrumpa las actividades institucionales ni comprometa la estabilidad del equipo.

Cada acción llevada a cabo durante la desinstalación debe quedar debidamente documentada, incluyendo el nombre del Software eliminado, fecha de intervención, equipo intervenido, nombre del técnico responsable y cualquier observación relevante. Esta documentación servirá como respaldo ante auditorías internas y facilitará el seguimiento en caso de incidentes futuros.

d) **Revisión de impacto**

Después de desinstalar el Software no autorizado, es indispensable realizar una revisión técnica para asegurarse de que la eliminación no haya afectado negativamente el funcionamiento general del sistema o de otras aplicaciones institucionales. Esta evaluación debe ser realizada por el personal de la Dirección de Servicios Tecnológicos, y tiene como objetivo garantizar la estabilidad, continuidad operativa y seguridad del equipo intervenido.

Durante esta revisión, se debe comprobar que no queden procesos del Software activo en segundo plano, servicios vinculados ejecutándose, o archivos residuales que puedan interferir con otras herramientas autorizadas. También se debe verificar que no existan dependencias rotas, es decir, funciones o componentes que otros programas necesitan para operar correctamente y que hayan sido alteradas o eliminadas en el proceso.

Además, el equipo técnico debe revisar el rendimiento general del sistema después de la desinstalación, prestando especial atención a posibles fallos, lentitud, errores de carga o conflictos con otras aplicaciones. Si se detecta algún problema derivado de la eliminación, se deberán aplicar las acciones correctivas necesarias de inmediato para restablecer el funcionamiento óptimo del equipo.

e) **Registro y seguimiento**

El incidente debe quedar documentado en la Bitácora de Software, conforme a lo indicado en el Anexo B. Este registro debe incluir detalles del Software eliminado, fecha, hora, responsables del procedimiento y las acciones realizadas. Además, se deben aplicar medidas para evitar que el Software vuelva a instalarse sin autorización, como ajustes en las configuraciones de red, restricciones de instalación o revisión de permisos de usuario.

Este seguimiento también debe contemplar una evaluación continua del cumplimiento de las políticas por parte de los usuarios, así como la actualización regular de la Bitácora de Software, de modo que se mantenga un control efectivo y actualizado sobre el uso del Software institucional

f) **Medidas preventivas**

Con el fin de reducir la reincidencia en el uso de Software no autorizado y fortalecer una cultura institucional basada en la responsabilidad y el cumplimiento, es necesario implementar medidas preventivas que actúen de manera proactiva sobre los usuarios y los sistemas tecnológicos.

Estas acciones pueden incluir, entre otras:

- **Bloqueo de instalaciones no autorizadas:** Configurar políticas de grupo (GPO) o herramientas de administración de sistemas que impidan a los usuarios instalar software sin la aprobación del área técnica. Esto garantiza que solo se pueda ejecutar software previamente validado;

- **Auditorías periódicas:** Realizar revisiones programadas en los dispositivos institucionales para detectar cualquier instalación irregular. Estas auditorías deben quedar documentadas y ser parte del control interno de la organización;

- **Restricciones de acceso:** Limitar los privilegios de instalación a usuarios reincidentes o a aquellos que hayan vulnerado las políticas previamente, impidiendo que realicen cambios en los sistemas sin supervisión técnica;

- **Capacitación continua:** Ofrecer talleres, sesiones informativas o recursos digitales que refuercen el conocimiento sobre las políticas de uso de Software autorizado, los riesgos del Software no permitido y las consecuencias administrativas de su instalación; y,

- **Recordatorios institucionales:** Enviar comunicaciones periódicas a todo el personal por correo institucional, carteles informativos o boletines internos recordando la importancia del cumplimiento de

las normas de seguridad tecnológica y la obligación de utilizar únicamente Software aprobado.

El propósito central de estas medidas es crear un entorno tecnológico seguro, confiable y alineado con las mejores prácticas de Ciberseguridad, donde cada usuario comprenda su responsabilidad en el uso correcto del Software y actúe de forma preventiva para proteger los activos institucionales.

VI. Responsabilidades

La Dirección de Servicios Tecnológicos y Plataforma Digital es responsable de coordinar el control y seguimiento del Software instalado en los activos tecnológicos, mantener actualizado el inventario de Software autorizado y excepciones, realizar revisiones periódicas para validar la vigencia de las excepciones, y ejecutar la eliminación segura del Software no autorizado dentro de la SESEA. Asimismo, junto con la Secretaría Técnica y la Delegación Administrativa, debe revisar y aprobar las solicitudes de excepciones, asegurando que estén justificadas y no representen riesgos para la operación institucional. Por su parte, la Delegación Administrativa válida licencias y garantiza que el Software utilizado cumpla con las políticas administrativas y presupuestales. Finalmente, los usuarios finales son responsables de utilizar únicamente Software autorizado, reportar necesidades especiales o problemas técnicos, y cumplir con las políticas institucionales sobre instalación, uso y eliminación de Software.

CAPÍTULO V
DE LA POLÍTICA PARA LA GESTIÓN DE DATOS

CIS CONTROL #3: PROTECCIÓN DE DATOS

I. **Propósito y Objetivo**

Establecer un marco normativo integral para la clasificación, manejo, almacenamiento y protección de los datos institucionales de la SESEA, con el propósito de salvaguardar la información como activo estratégico de la organización y garantizar el cumplimiento de las obligaciones legales en materia de transparencia, acceso a la información y protección de datos personales.

En esta política se busca implementar controles diferenciados de seguridad según la naturaleza y sensibilidad de la información, asegurando que cada tipo de dato reciba el tratamiento adecuado para preservar su confidencialidad, integridad y disponibilidad. Asimismo, pretende fortalecer la capacidad operativa institucional mediante la gestión eficiente de los recursos de información, manteniendo la confianza ciudadana en los procesos anticorrupción y garantizando la continuidad de las funciones sustantivas de la SESEA.

A través de la aplicación de estos lineamientos, se busca establecer criterios claros para la identificación, categorización y manejo de datos institucionales, definir niveles apropiados de acceso y protección, y promover una cultura de responsabilidad en el manejo de la información entre las personas servidoras públicas de la SESEA.

II. **Alcance**

Esta política aplica a todos las personas servidoras públicas, áreas, sistemas y procesos de la SESEA que manejan, almacenan o tienen acceso a datos institucionales, independientemente del formato o medio en que se encuentren ya sea digital, físico o verbal. Cubre todas las etapas del ciclo de vida de la información, desde su generación, clasificación, uso, almacenamiento, transferencia y protección, hasta su disposición final. Asimismo, incluye la implementación de controles de seguridad diferenciados según la sensibilidad de la información, así como la definición de roles y responsabilidades para garantizar el cumplimiento de

las obligaciones legales en materia de transparencia, acceso a la información y protección de datos personales.

III. **Descripción de la política**

Esta política establece las directrices para el manejo adecuado de los datos institucionales en la SESEA, considerando su valor estratégico y el cumplimiento de los marcos normativos aplicables. Para ello, se definen cinco elementos clave que deben guiar su gestión: la categoría de los datos, que se refiere al tipo de información que se gestiona en la SESEA , la clasificación de los datos, que consiste en organizarlos según su nivel de sensibilidad y el riesgo asociado a su divulgación no autorizada, el almacenamiento de los datos, que implica resguardarlos adecuadamente conforme a su nivel de clasificación y con los controles de seguridad necesarios; la retención de los datos, que establece el tiempo que deben conservarse de acuerdo con su utilidad o requerimientos legales; y, finalmente, la eliminación de los datos, que debe realizarse de forma segura y controlada una vez que la información ha cumplido su ciclo de vida institucional.

IV. **Categoría de datos**

Se han identificado las siguientes categorías de datos que requieren tratamiento especializado dentro del marco institucional de la SESEA:

a) **Datos personales sensibles.** Información que revela origen étnico, opiniones políticas, creencias religiosas, estado de salud, datos biométricos, orientación sexual, entre otros, que requieren protección especial para evitar discriminación o daños;

b) **Datos personales generales.** Información de identificación como nombre, dirección, teléfono, correo electrónico, CURP, RFC, que deben protegerse para evitar su uso indebido o robo de identidad;

c) **Datos financieros.** Información sobre cuentas bancarias, movimientos financieros, pagos y cualquier dato económico que pueda afectar la privacidad o seguridad financiera de personas o la SESEA;

d) **Información confidencial de investigaciones.** Datos relacionados con casos de corrupción, investigaciones internas o auditorías que deben mantenerse bajo estricta reserva para proteger la integridad del proceso;

e) **Información estratégica o clasificada.** Datos que impactan la seguridad institucional, como planes operativos, procedimientos internos, sistemas de control o información reservada que pueda poner en riesgo la misión de la SESEA;

f) **Datos de acceso y control.** Credenciales, contraseñas, registros de acceso a sistemas y otros datos que permiten controlar el uso de recursos tecnológicos y que requieren protección para evitar accesos no autorizados;

g) **Datos jurídicos y contractuales.** Información sobre contratos, acuerdos legales, licitaciones y documentos jurídicos que deben conservarse con confidencialidad para proteger intereses institucionales y cumplir con normativas legales.

Estos tipos de datos demandan medidas específicas de seguridad, control de acceso y tratamiento conforme a la legislación vigente y a las políticas internas de la SESEA;

h) **Datos públicos institucionales.** Son aquellos datos generados, administrados o custodiados por la SESEA que, por ley o por mandato de transparencia, deben estar disponibles para el acceso público. Aunque no requieren medidas de confidencialidad, sí deben mantenerse completos, actualizados y accesibles para cumplir con las obligaciones de rendición de cuentas. Su gestión implica garantizar que se publiquen de manera oportuna, en formatos abiertos y con mecanismos que aseguren su integridad y fácil consulta.

Ejemplos: información presupuestal, estructura orgánica, directorios, informes de actividades, reportes de metas, contratos públicos, declaraciones patrimoniales en versiones públicas, actas de sesión y estadísticas institucionales;

i) **Clasificación de Datos.** La clasificación de datos es el proceso mediante el cual se organizan y etiquetan los datos según su nivel de sensibilidad y el posible impacto que tendría su divulgación no autorizada. Esto permite aplicar medidas de seguridad adecuadas y proporcionales al valor y riesgo asociado a cada tipo de información, se clasifican de acuerdo a la siguiente tabla:

Nivel de Sensibilidad	Descripción	Ejemplos
Alta (Confidencial)	Su divulgación puede causar daño legal o institucional	Datos personales, contraseñas, registros médicos, información financiera
Media (Interno restringido)	Uso exclusivo de áreas específicas. Divulgación afecta operaciones	Manuales internos, reportes de gestión.
Baja (Público o compartido)	Su eliminación no compromete la seguridad o confidencialidad	Documentos públicos, material de difusión, formularios genéricos

j) **Almacenamiento de Datos.** El almacenamiento de los datos institucionales debe realizarse de manera segura, ordenada y conforme a su nivel de sensibilidad. Para proteger adecuadamente la información, es necesario aplicar medidas técnicas y organizativas que garanticen su confidencialidad, integridad y disponibilidad. Entre estas medidas se incluyen:

1. **Control de Acceso.** El control de acceso es un mecanismo fundamental para proteger los datos institucionales, ya que permite limitar quién puede ver, modificar o gestionar cierta información dentro de la organización. Para ello, se recomienda aplicar un modelo de control basado en roles (RBAC, por sus siglas en inglés), el cual asigna permisos a los usuarios en función de su puesto, funciones o nivel de responsabilidad dentro de la SESEA. Esto significa que cada persona sólo podrá acceder a los datos necesarios para cumplir con sus tareas, y no a toda la información institucional.

Este modelo ayuda a reducir el riesgo de accesos no autorizados, errores humanos o mal uso de la información. Además, facilita la trazabilidad, ya que se puede identificar fácilmente quién accedió a qué información, en qué momento y con qué propósito. Todo acceso debe ser revisado y validado periódicamente para asegurar que los permisos asignados continúan siendo apropiados;

2. **Cifrado.** El cifrado es una medida fundamental de seguridad que protege la información mediante su codificación, de modo que sólo puede ser leída o utilizada por personas o sistemas autorizados que cuenten con la clave adecuada para descifrarla. Este proceso es especialmente importante cuando se trata de datos confidenciales o altamente confidenciales, como información personal sensible, datos financieros o documentos estratégicos.

   El cifrado debe aplicarse en dos momentos clave:

   2.1 **En reposo:** cuando los datos están almacenados en discos duros, servidores, bases de datos o dispositivos externos. Cifrar los datos en reposo evita que, en caso de pérdida, robo o acceso físico no autorizado, la información pueda ser leída o utilizada de forma indebida; y,

   2.2 **En tránsito:** cuando los datos se envían a través de redes, ya sea por correo electrónico, transferencias de archivos o conexiones entre sistemas. Cifrar la información en tránsito protege contra interceptaciones, evitando que un tercero pueda espiar o modificar los datos mientras se transfieren.

   Implementar el cifrado garantiza la confidencialidad e integridad de la información, reduciendo el riesgo de filtraciones, accesos no autorizados o manipulación de datos. Además, contribuye al cumplimiento de normativas legales y estándares de seguridad institucional.

3. **Respaldo.** Es indispensable realizar copias de seguridad periódicas y almacenarlas en una ubicación segura, distinta de la ubicación principal, para garantizar la recuperación de información en caso de pérdida o incidente;

4. **Integridad.** La integridad asegura que los datos sean precisos y no se modifiquen de forma no autorizada o accidental. Para protegerla, se implementan controles como reglas de validación al ingresar datos, registros de accesos y cambios, y auditorías periódicas. Esto garantiza que la información sea confiable y se mantenga fiel a su estado original; y,

5. **Ubicación.** Los datos deben almacenarse en lugares físicos y digitales que ofrezcan un nivel adecuado de seguridad para protegerlos contra accesos no autorizados, pérdida, robo o daños. Esto implica elegir centros de datos o instalaciones que cuenten con medidas de seguridad físicas robustas, como controles de acceso restringido, vigilancia continua y sistemas contra incendios. Además, estas ubicaciones deben cumplir con las normativas legales y reglamentarias aplicables, como las leyes de protección de datos personales, normativas de transparencia, regulaciones sectoriales y estándares internacionales de seguridad que pueden incluir requisitos específicos sobre dónde se pueden alojar ciertos tipos de datos, especialmente cuando se trata de información sensible o personal. De esta manera, se garantiza no solo la protección física y lógica de la información, sino también el cumplimiento de las obligaciones legales vigentes.

Estas prácticas permiten reducir riesgos asociados al acceso no autorizado, pérdida, corrupción o mal uso de la información, fortaleciendo la seguridad institucional y el cumplimiento de la normativa vigente;

k) **Retención de Datos.** La retención de datos es el proceso de determinar por cuánto tiempo se deben guardar los datos antes de eliminarlos de forma segura. Este tiempo dependerá de dos factores principales:

1. **Leyes y regulaciones vigentes**, que indican cuánto tiempo deben conservarse ciertos tipos de información (por ejemplo, datos fiscales, contratos o datos personales);

2. **Políticas internas de la SESEA**, las cuales definen reglas específicas para el manejo, conservación y eliminación de la

información institucional, como lo establecido en la *Política de plazos mínimos y máximos de conservación de datos; y,*

l) **Eliminación Segura de Datos.** La eliminación de datos consiste en borrar o destruir la información de forma segura cuando ya ha cumplido su propósito o ha expirado el período de retención establecido. Este proceso es fundamental por varias razones: permite liberar espacio de almacenamiento, evitando la acumulación innecesaria de información y optimizando el uso de los recursos tecnológicos; reduce riesgos de seguridad al eliminar datos que podrían ser vulnerables a accesos no autorizados o filtraciones; y garantiza el cumplimiento de las disposiciones legales y normativas, como las leyes de protección de datos personales y las obligaciones en materia de transparencia, que exigen eliminar ciertos tipos de información una vez que ya no son necesarios para fines institucionales. La eliminación de datos debe realizarse mediante métodos seguros que impidan su recuperación, tanto si se trata de información digital como en formato físico. Este proceso debe ajustarse a la clasificación de los datos y seguir procedimientos específicos, como los siguientes:

V. **Datos en Papel:**

Para garantizar la eliminación de datos en papel, es necesario aplicar técnicas que impidan cualquier posibilidad de recuperación, Entre estas técnicas se incluyen:

a) **Trituración.** Los documentos en papel que contienen datos confidenciales o altamente confidenciales deben ser triturados utilizando una trituradora de papel que cumpla con los estándares de seguridad adecuados. La trituración debe realizarse de manera que los datos sean ilegibles e irrecuperables.

La norma más utilizada internacionalmente para clasificar la seguridad de las trituradoras de papel es la norma DIN 66399. Esta norma clasifica los materiales a destruir en diferentes categorías y define siete niveles de seguridad (P1 a P7) para la trituración de papel, donde:

P-1: Material general (por ejemplo, documentos que no son sensibles);

P-2: Material confidencial (por ejemplo, correspondencia interna);
P-3: Material especialmente confidencial (por ejemplo, datos personales);
P-4: Material secreto (por ejemplo, documentos que contienen datos protegidos)
P-5: Material de alto secreto
P-6: Máximo secreto; y,
P-7: Máxima alta confidencialidad (seguridad más exigente).

b) **Destrucción Certificada.** En casos donde se maneje un gran volumen de documentos confidenciales, se puede contratar a un proveedor de servicios de destrucción de documentos certificados, que garantice la eliminación segura y la entrega de un certificado de destrucción.

VI. **Datos Electrónicos:**

Para garantizar la eliminación segura de datos en discos duros y otros medios de almacenamiento, es necesario aplicar técnicas que impidan cualquier posibilidad de recuperación. Entre estas técnicas se incluyen:

a) **Sobrescritura.** Consiste en utilizar Software especializado que reescribe varias veces la información almacenada en discos duros, unidades de estado sólido (SSD), memorias USB u otros dispositivos. Este proceso reemplaza los datos originales con información aleatoria, lo que dificulta o impide su recuperación;

b) **Desmagnetización.** Aplicable a medios de almacenamiento magnéticos, como discos duros tradicionales o cintas magnéticas. Este procedimiento utiliza un campo magnético potente para borrar completamente los datos eliminando las señales almacenadas. Es importante señalar que, una vez desmagnetizado, el dispositivo queda inutilizable;

c) **Destrucción Física.** Cuando no es posible borrar los datos mediante Software o desmagnetización, se debe recurrir a la destrucción física del dispositivo. Esto puede incluir la trituración, perforación, incineración o cualquier método que garantice que el medio no pueda ser reutilizado ni los datos recuperados; y,

d) **Cifrado previo al desecho (opcional).** Aunque el medio físico vaya a ser eliminado, es recomendable que toda la información contenido haya sido previamente cifrada, esto con el fin de prevenir accesos no autorizados en cualquier etapa del ciclo de vida de dicho medio. Para poder cifrar la información contenida se proponen las siguientes herramientas:

Herramienta	Sistema compatible	Tipo de cifrado
BitLocker	Windows	Cifrado por volumen
VeraCrypt	Windows, Linux, macOS	Cifrado de archivos o discos
LUKS	Linux	Cifrado de particiones

VII. Métodos de Eliminación según el nivel de Sensibilidad de los datos

a) **Datos de Alta Sensibilidad (Confidencial).** La información clasificada como de alta sensibilidad incluye aquellos datos cuya divulgación no autorizada podría generar consecuencias legales, financieras, operativas o reputacionales para la SESEA, por lo que su eliminación debe ser irreversible y verificable.

El método obligatorio para su eliminación es el borrado seguro mediante sobreescritura. Se recomienda una sobrescritura mínima de tres pasadas, conforme al estándar DoD 5220.22-M (idealmente con siete pasadas). Para garantizar su efectividad, la eliminación debe ejecutarse en un ambiente controlado, capturar evidencia del proceso (como logs o capturas de pantalla) y documentarse en la bitácora oficial de eliminación;

b) **Datos de Media Sensibilidad (Interno restringido).** Los datos clasificados como de sensibilidad media son aquellos cuya exposición no representa un riesgo tan alto como los de alta sensibilidad, pero cuya protección sigue siendo importante para el funcionamiento interno de la SESEA. Por ello, se recomiendan métodos de eliminación menos estrictos, pero aún controlados, como el formateo completo del dispositivo (no rápido), la reinstalación del sistema con limpieza de

particiones, o un borrado lógico con una sola pasada de sobrescritura. En algunos casos, si se considera viable, el dispositivo puede ser reubicado para su reutilización interna, siempre y cuando cuente con la validación previa de la Dirección de Servicios Tecnológicos y Plataforma Digital, asegurando así que no existan riesgos de recuperación indebida de la información; y,

c) **Datos de Baja Sensibilidad (Público o compartido).** Este tipo de información, al no representar un riesgo significativo en caso de exposición, permite el uso de métodos de eliminación simples. Los datos pueden eliminarse mediante mecanismos convencionales, como el envío a la papelera de reciclaje o el formateo rápido del dispositivo. Aunque no se requiere el uso de Software especializado, es indispensable que el usuario responsable realice una verificación visual para asegurarse de que los datos han sido efectivamente eliminados y que no quedan copias residuales en el sistema o dispositivo.

VIII. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de implementar los controles necesarios para garantizar el almacenamiento, acceso y eliminación segura de los datos institucionales, de acuerdo con su clasificación. También debe coordinar la aplicación de medidas técnicas como cifrado, respaldos y control de acceso, así como apoyar en la eliminación segura de datos cuando estos hayan cumplido su periodo de retención.

La Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales tiene la responsabilidad de asegurar que la gestión de datos cumpla con las obligaciones establecidas en la Ley General de Transparencia y Acceso a la Información Pública, asesorando sobre qué datos deben mantenerse disponibles y cuáles deben clasificarse como reservados o confidenciales, así como participar en la definición de plazos de conservación relacionados con obligaciones de publicación.

Esta Unidad también es responsable de supervisar que el tratamiento de datos personales se realice conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, asesorando a las áreas en su correcta clasificación, almacenamiento y disposición final.

La Dirección de Normatividad y Asuntos Jurídicos debe definir los requisitos legales y regulatorios aplicables al tratamiento, retención y eliminación de los datos, incluyendo los plazos establecidos en normativas locales y nacionales. Asimismo, debe proporcionar asesoría para garantizar que los datos sean tratados conforme a la legislación vigente y sin comprometer los intereses legales de la SESEA.

El Órgano Interno de Control (OIC) debe verificar el cumplimiento de esta política mediante auditorías o revisiones internas, supervisar el adecuado seguimiento de los procedimientos establecidos para la gestión de datos y emitir observaciones o recomendaciones ante incumplimientos.

Por su parte, los propietarios de los datos (aquellas áreas o unidades que generan o administran información) son responsables de clasificar los datos conforme a su nivel de sensibilidad, definir los periodos de retención, garantizar su correcta conservación durante su ciclo de vida y solicitar su eliminación segura una vez que hayan cumplido su función institucional.

Finalmente, todos los usuarios institucionales tienen la responsabilidad de manejar los datos conforme a las políticas establecidas, respetar los controles de acceso, reportar incidentes de seguridad y contribuir al cumplimiento de las disposiciones sobre protección de información, transparencia y uso adecuado de los datos.

IX. **Procedimiento para la eliminación segura de datos.**

La eliminación de datos en la SESEA debe realizarse de forma segura y controlada, siguiendo una metodología estructurada que garantice que los datos no puedan ser recuperados y que cada paso del proceso quede debidamente documentado. A continuación, se explica cada etapa a seguir:

a) **Identificación y Clasificación del Dato.** El usuario que solicita la eliminación, en conjunto con la Dirección de Servicios Tecnológicos, debe identificar el tipo de información y clasificarla según su nivel de sensibilidad (alta, media o baja). Esta clasificación determina qué método de eliminación se aplicará;

b) **Selección del Método de Eliminación.** La Dirección de Servicios Tecnológicos analiza el medio de almacenamiento (por ejemplo, disco duro, USB, cinta magnética) y el tipo de datos para elegir el método más

adecuado. Esta decisión considera aspectos como la confidencialidad de la información y los estándares de seguridad vigentes;

c) **Ejecución del Proceso.** Personal autorizado y capacitado de la Dirección de Servicios Tecnológicos realiza la eliminación de los datos, utilizando herramientas y procedimientos previamente definidos. Esta acción debe realizarse bajo supervisión directa para garantizar su correcta ejecución;

d) **Documentación del Proceso:** La persona responsable de la eliminación de los datos y su supervisor registran la acción ejecutada en el formato de eliminación, creando una bitácora que incluye todos los elementos requeridos para la trazabilidad y auditoría posterior del proceso;

e) **Verificación y Validación:** Un revisor ajeno confirma que la eliminación se ejecutó correctamente, verificando que no existen datos residuales recuperables y que los medios de almacenamiento no presentan riesgos de reutilización inadecuada;

f) **Datos en la Nube.** Cuando la información institucional se almacena en servicios en la nube, su eliminación debe realizarse utilizando los mecanismos seguros que ofrezca el proveedor. Es fundamental asegurarse de que estos métodos garanticen que los datos no puedan ser recuperados posteriormente y que el proveedor cumpla con los estándares de seguridad establecidos en normativas aplicables. Además, los contratos con proveedores de servicios en la nube deben incluir cláusulas específicas sobre los procedimientos de eliminación de datos, así como las responsabilidades del proveedor en caso de pérdida, filtración o acceso no autorizado a la información. Esto asegura una gestión adecuada y segura de los datos incluso fuera de los entornos tecnológicos internos de la SESEA.

X. **Baja de Sistemas.**

a) **Planificación de la Baja:** Antes de dar de baja un sistema (servidor, estación de trabajo, dispositivo móvil, entre otros.) que almacena o procesa datos, se debe elaborar un plan de baja que detalle los pasos a seguir para eliminar los datos de forma segura y garantizar que no se comprometa la confidencialidad de la información;

b) **Identificación de Datos:** Antes de dar de baja un sistema, es fundamental identificar de forma exhaustiva todos los datos que contiene. Esto incluye información del sistema operativo, bases de datos, archivos de aplicaciones, documentos generados por los usuarios, configuraciones, respaldos y cualquier otro tipo de dato sensible o institucional. Esta identificación permite garantizar que ningún dato relevante permanezca sin ser gestionado adecuadamente, ya sea para su migración, respaldo o eliminación segura, conforme a los lineamientos establecidos por la SESEA y las obligaciones legales en materia de protección de datos;

c) **Métodos de Eliminación:** Los sistemas dados de baja deben ser tratados conforme a la *Política para la Eliminación del Software No Autorizado*. Esto implica aplicar métodos de eliminación segura adecuados según la clasificación de los datos contenidos. Entre estos métodos se incluyen la sobreescritura de discos duros mediante Software especializado, la desmagnetización de medios magnéticos y, en casos donde no sea posible una eliminación lógica segura, la destrucción física del hardware (como trituración o perforación). Estos procedimientos aseguran que la información institucional no pueda ser recuperada, reduciendo riesgos de seguridad y garantizando el cumplimiento de las normativas vigentes en materia de protección de datos;

d) **Verificación de la Eliminación:** Una vez completado el proceso de eliminación, es fundamental realizar una verificación para confirmar que los datos han sido eliminados correctamente y que no pueden ser recuperados por ningún medio. Esta validación puede incluir el uso de herramientas de análisis forense o Software de verificación para asegurar que no queden rastros accesibles de la información. El objetivo es garantizar que la eliminación fue efectiva, especialmente cuando se trata de datos sensibles o confidenciales, reduciendo así el riesgo de filtraciones o accesos no autorizados posteriores;

e) **Documentación de la Baja:** Se debe documentar el proceso de baja del sistema, incluyendo: Fecha de la baja, descripción del sistema dado de baja, identificación de los datos almacenados en el sistema, métodos de eliminación de datos utilizados, resultados de la verificación de la eliminación y nombre de la persona responsable de la baja; y,

f) **Custodia del Hardware:** El hardware que haya sido dado de baja deberá ser entregado al Departamento de Recursos Humanos, Financieros y Materiales de la Delegación Administrativa, la cual será responsable de mantenerlo bajo resguardo en un lugar seguro y con acceso controlado, hasta que se lleve a cabo su disposición final (como destrucción física, reciclaje o donación). Asimismo, se deberá llevar un registro detallado que documente el destino final del equipo, incluyendo la fecha de baja, el método de disposición utilizado y los responsables del proceso. Esto permite garantizar la trazabilidad, la rendición de cuentas y la seguridad de los activos tecnológicos hasta su eliminación definitiva.

CAPÍTULO VI
DE LA POLÍTICA ACERCA DEL INVENTARIO DE DATOS

CIS CONTROL #3: PROTECCIÓN DE DATOS

I. **Propósito y Objetivo**

Establecer un sistema integral de inventario y registro de datos que permita a la SESEA mantener un control efectivo sobre toda la información que genera, recopila, procesa, almacena y comparte en el ejercicio de sus funciones institucionales.

Esta política tiene como propósito implementar mecanismos de identificación, clasificación y monitoreo continuo de los activos de información institucional, garantizando la trazabilidad completa de los datos desde su origen hasta su disposición final. A través de la aplicación de estos lineamientos, se busca fortalecer las capacidades de gestión informacional de la SESEA y asegurar el cumplimiento de las obligaciones normativas aplicables.

II. **Alcance**

Esta política aplica a todos los datos institucionales generados, recibidos, procesados, almacenados o compartidos por cualquier área, sistema, proceso o persona servidora pública de la SESEA, independientemente del formato (físico o digital) y del medio en que se encuentren.

Incluye tanto los datos operativos, administrativos, personales, financieros, estratégicos y públicos, como aquellos que se encuentran en sistemas internos, plataformas digitales, servicios en la nube o archivos físicos. Asimismo, abarca todo el ciclo de vida de la información: desde su creación o recopilación, clasificación, uso, resguardo, actualización y transferencia, hasta su baja o eliminación definitiva. Esta política también establece la obligación de todas las unidades administrativas de identificar y registrar los activos de datos bajo su responsabilidad, mantenerlos actualizados y aplicar las medidas correspondientes para asegurar su integridad, confidencialidad, disponibilidad y trazabilidad. La implementación de esta política es obligatoria para todo el personal de la SESEA que intervenga directa o indirectamente en el manejo de datos institucionales.

III. **Descripción de la política**

Esta política establece que cada unidad administrativa de la SESEA debe identificar y registrar todos los datos que genera y utiliza, creando un inventario detallado que facilite su gestión y protección.

Además, este inventario debe actualizarse periódicamente para reflejar cualquier cambio en la información, asegurando así la trazabilidad y el control continuo de los datos.

IV. **Actualización de datos**

La Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emitirá al menos dos veces al año un oficio dirigido a todas las unidades administrativas de la SESEA, con el fin de actualizar sus inventarios de datos. En dicho oficio se establecerán los plazos y requisitos específicos para la revisión y actualización de la información correspondiente a los datos bajo su custodia. Esta notificación incluirá los formatos estandarizados, criterios de clasificación y procedimientos técnicos necesarios para garantizar la homogeneidad en el proceso de actualización.

Por su parte, las unidades administrativas de la SESEA tienen la obligación de informar de manera inmediata a la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales sobre cualquier modificación sustancial en sus procesos de datos, o bien, cuando implementen nuevas tecnologías que afecten el tratamiento de datos institucionales, como lo son:

a) **La integración de nuevos sistemas:** Se refiere a la implementación de nuevas plataformas, aplicaciones o herramientas tecnológicas destinadas al manejo de información institucional, como puede ser un sistema de gestión documental, de seguimiento de trámites, control de expedientes, entre otros. Estos sistemas pueden modificar la forma en que se recopilan, almacenan, procesan o comparten los datos;

b) **Cambios en sistemas:** Se refiere a cualquier modificación importante en un sistema tecnológico ya existente que afecte el manejo de la información. Por ejemplo, la incorporación de nuevas funcionalidades que impliquen la recolección de datos adicionales, cambios en los

procesos de almacenamiento o actualización de los métodos de procesamiento de información;

c) **Nuevos procesos:** Se refiere a la implementación de procesos de trabajo nuevos o modificados que involucran la creación, recopilación o utilización de datos que antes no se manejaban. Esto puede incluir, por ejemplo, nuevos procedimientos administrativos, formularios digitales o flujos de trabajo que generan o requieren información adicional;

d) **Cambios en las leyes:** Se refiere a cualquier modificación en la legislación vigente que obligue a ajustar o modificar el funcionamiento estándar de los sistemas de la SESEA. Esto puede incluir actualizaciones para cumplir con nuevas disposiciones legales en materia de protección de datos, transparencia o seguridad de la información; y,

e) **Nuevos tipos de datos:** Se refiere a cuando la SESEA empieza a gestionar o procesar tipos de información que antes no formaban parte de sus actividades habituales. Esto puede incluir datos adicionales o diferentes en naturaleza, origen o sensibilidad, lo que requiere actualizar los inventarios, medidas de protección y controles para asegurar un manejo adecuado conforme a las políticas institucionales y normativas vigentes.

V. Mantenimiento del Inventario

El inventario de datos se mantendrá en una plataforma digital que garantice la consulta eficiente, actualización oportuna y generación de reportes automatizados. El sistema contará con controles de acceso basados en roles y perfiles de usuario, asegurando que únicamente el personal debidamente autorizado pueda consultar o modificar la información del inventario según sus competencias y responsabilidades institucionales.

VI. Revisión Periódica del Inventario

El inventario de datos será sometido a una revisión integral anual, conducida por el Comité de Transparencia. En esta verificación se evaluará la pertinencia, actualidad y efectividad del inventario, identificando oportunidades de mejora en los procesos

de gestión de datos y proponiendo ajustes normativos o tecnológicos que fortalezcan el sistema de información institucional.

CAPÍTULO VII
DE LA POLÍTICA PARA APLICAR CONTROLES DE ACCESO A DATOS

CIS CONTROL #3: PROTECCIÓN DE DATOS

I. **Propósito y Objetivo**

Esta política establece las reglas y procedimientos para gestionar y controlar el acceso a la información digital de la SESEA. Su objetivo es asegurar que solo el personal autorizado y con una razón válida pueda acceder a datos específicos, de acuerdo con sus funciones y responsabilidades. Así, se busca reducir al mínimo los riesgos de accesos no autorizados, uso indebido o divulgación inapropiada de información confidencial. Para lograrlo, se aplicarán principios de seguridad como el “necesidad de saber” (acceder solo a la información necesaria para el trabajo) y el “mínimo privilegio” (otorgar sólo los permisos estrictamente necesarios), fortaleciendo la protección general de la información institucional.

II. **Alcance**

Esta política aplica a todas las personas servidoras públicas, contratistas y terceros que tengan acceso a sistemas, aplicaciones y bases de datos digitales de la SESEA. Cubre cualquier tipo de información institucional almacenada, procesada o transmitida en formato digital, sin importar el dispositivo o plataforma utilizada. Incluye el acceso a datos personales, financieros, estratégicos, confidenciales y públicos, así como a los sistemas que los gestionan. Además, establece las responsabilidades para la asignación, revisión y revocación de permisos de acceso, asegurando que dichos controles estén alineados con las funciones y niveles de responsabilidad de cada usuario, garantizando la protección y correcta gestión de la información en todas las etapas de su ciclo de vida.

III. **Descripción de la política**

Esta política establece un marco integral para la gestión y control del acceso a la información digital en la SESEA, basado en los principios de *Necesidad de Saber* y *Mínimo Privilegio*. El acceso a la información se otorga exclusivamente a quienes requieren la información para cumplir con sus responsabilidades laborales,

limitando el acceso al mínimo indispensable para el desempeño efectivo de sus funciones.

Para garantizar la seguridad de la información, se implementan controles técnicos, administrativos y físicos que permiten autenticar usuarios, autorizar accesos según perfiles predefinidos y registrar todas las actividades relacionadas con la información institucional. Esta gestión se fundamenta en principios rectores como acceso restrictivo, responsabilidad individual, revisión periódica de permisos y trazabilidad completa de las acciones.

IV. **Principios Rectores**

La gestión del acceso a los datos en la SESEA se basa en los principios fundamentales que garantizan la seguridad y buen manejo de la información siguientes:

a) **Acceso Restrictivo:** Solo se permite el acceso a la información a aquellas personas que hayan demostrado una necesidad legítima y justificada, de acuerdo con sus funciones. Esto asegura que nadie pueda acceder a datos innecesarios para su trabajo, minimizando riesgos de exposición indebida;

b) **Mínimo Privilegio:** A cada usuario se le otorgan únicamente los permisos estrictamente necesarios para realizar sus tareas específicas. De esta forma, se evita que tengan acceso a información o funciones que no requieren, limitando potenciales errores o mal usos;

c) **Responsabilidad Individual:** Cada persona servidora pública es responsable de cuidar y utilizar correctamente la información que tiene bajo su custodia. Esto implica manejarla con confidencialidad, integridad y conforme a las políticas y normativas vigentes;

d) **Revisión Continua:** Se realizan evaluaciones periódicas para verificar que los accesos otorgados sigan siendo pertinentes y adecuados según los cambios en funciones o estructuras organizacionales, de acuerdo a lo indicado en la *Política para el uso correcto de cuentas y privilegios de acceso, principio de privilegio mínimo*. Esto garantiza que los permisos no queden obsoletos o inapropiados con el tiempo; y,

e) **Trazabilidad Completa:** Todas las acciones relacionadas con el acceso a la información incluyendo consultas, modificaciones o transferencias quedan registradas con su justificación correspondiente. Esto facilita auditorías, detección de incidentes y asegura la transparencia en el manejo de datos.

V. Implementación del Marco de Control Digital

La aplicación estricta del principio de necesidad de saber es esencial para minimizar los riesgos de acceso no autorizado a datos confidenciales. Esta práctica fortalece la seguridad informática institucional al garantizar que únicamente el personal autorizado, con un propósito legítimo, acceda a la información sensible. Así, se protege la integridad y confidencialidad de los datos, además de asegurar el cumplimiento de las normativas legales vigentes en materia de protección de datos personales.

Como apoyo a esta política, el Anexo C del presente Manual incluye la Matriz de Clasificación de Datos. Esta herramienta proporciona una descripción detallada de la información gestionada por cada área organizacional, indicando los tipos de datos, su ubicación física y digital, las medidas de seguridad implementadas y los controles de acceso específicos aplicables a cada categoría de información, facilitando un manejo adecuado y seguro de los activos informacionales.

VI. Responsabilidades

a) **Custodios de Información:** Son los responsables directos de la información dentro de su área. Deben clasificar adecuadamente los datos bajo su custodia, definir quiénes pueden acceder a ellos y autorizar el acceso únicamente cuando exista una necesidad funcional justificada. Además, deben garantizar que los niveles de acceso asignados correspondan con la sensibilidad de la información;

b) **Jefes de Área:** Tienen la tarea de supervisar que esta política se cumpla dentro de sus respectivos equipos o departamentos. Esto incluye revisar de manera periódica los permisos de acceso otorgados a su personal para asegurar que sean apropiados y estén actualizados. Asimismo,

deben reportar cualquier incidente o irregularidad en la seguridad relacionada con el acceso a la información;

c) **Dirección de Servicios Tecnológicos y Plataforma Digital:** Es responsable de poner en marcha y mantener los mecanismos técnicos necesarios para controlar y proteger el acceso a los sistemas de información. Esto implica administrar los sistemas que gestionan los permisos de acceso y generar reportes de auditoría para monitorear el uso correcto y seguro de la información institucional;

d) **La Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales** es responsable de asesorar sobre el cumplimiento de las normativas de transparencia y protección de datos, asegurando que los accesos y tratamientos de información cumplan con los requerimientos legales aplicables; y,

e) **Personal en General:** Todas las personas servidoras públicas y colaboradores deben cumplir estrictamente con las normas establecidas en esta política. Deben utilizar la información únicamente para los fines autorizados, protegerla adecuadamente y reportar de inmediato cualquier anomalía o intento de acceso no autorizado que detecten, contribuyendo así a la seguridad global de los datos.

CAPÍTULO VIII
DE LA POLÍTICA DE PLAZOS MÍNIMOS Y MÁXIMOS DE CONSERVACIÓN DE DATOS

CIS CONTROL #3: PROTECCIÓN DE DATOS

I. **Propósito y Objetivo**

Esta política tiene como finalidad establecer los plazos mínimos y máximos para la conservación de los datos en la SESEA. Busca asegurar una gestión eficiente y ordenada del ciclo de vida de la información, desde su generación y uso hasta su eliminación definitiva. Al definir estos plazos, se pretende evitar la acumulación innecesaria de datos que pueda generar riesgos legales, de seguridad o administrativos, y al mismo tiempo garantizar que la información esté disponible y accesible cuando sea necesaria para cumplir con obligaciones legales, operativas o de transparencia.

II. **Alcance**

Esta política es aplicable a todas las unidades administrativas, personas servidoras públicas, contratistas y terceros que gestionan, almacenan o procesan datos en la SESEA. Cubre todos los tipos de datos generados, recibidos o administrados en formato digital o físico, independientemente de su naturaleza (personal, financiera, operativa, estratégica, confidencial o pública).

Asimismo, establece las responsabilidades para la correcta aplicación, seguimiento y cumplimiento de los plazos mínimos y máximos de conservación, así como para la disposición final o eliminación segura de los datos conforme a las normativas vigentes y los procedimientos internos institucionales.

III. **Descripción de la política**

Esta política establece los criterios y lineamientos para determinar los plazos mínimos y máximos durante los cuales la SESEA debe conservar sus datos e información institucional, garantizando una gestión adecuada y ordenada del ciclo de vida de los datos desde su generación hasta su disposición final.

Para definir los plazos de conservación, la política considera varios factores clave:

a) **Requisitos Legales y Reglamentarios:** Se toman en cuenta las disposiciones legales y normativas vigentes que establecen periodos específicos para conservar ciertos tipos de datos, tales como información fiscal, laboral, o datos personales protegidos, asegurando así el cumplimiento de las obligaciones legales y evitando sanciones o responsabilidades;

b) **Necesidades Operativas:** Se evalúa el tiempo durante el cual los datos son necesarios para el correcto funcionamiento institucional, incluyendo el soporte a actividades administrativas, operativas, toma de decisiones y prestación de servicios, garantizando que la información esté disponible cuando sea requerida para fines legítimos;

c) **Obligaciones Contractuales:** Se consideran los términos y condiciones establecidos en contratos con terceros, que pueden especificar plazos particulares para conservar la información vinculada a la relación contractual, asegurando el cumplimiento de compromisos pactados;

d) **Riesgos Asociados:** Se analizan los riesgos que implica la retención prolongada de datos, tales como vulnerabilidades de seguridad, pérdida de confidencialidad, o responsabilidades legales derivadas del almacenamiento innecesario de información sensible;

e) **Nivel de Confidencialidad:** Se reconoce que la naturaleza y sensibilidad de los datos influyen directamente en la duración de su conservación y en los métodos utilizados para su eliminación segura de acuerdo a la *Política para la Gestión de Datos*, protegiendo así la privacidad y la integridad de la información institucional;

f) **Plazos de Conservación de Datos.** Los plazos mínimos y máximos para conservar los datos generados, recibidos o administrados por la SESEA están establecidos en la Matriz de Clasificación de Datos contenida en el Anexo C de esta política. Dicha matriz determina el tiempo durante el cual cada tipo de información debe mantenerse disponible antes de ser transferida a archivo definitivo o eliminada de forma segura de acuerdo a la Política para la Gestión de datos.

Esta clasificación se basa en los instrumentos normativos oficiales de gestión documental de la SESEA, específicamente:

1. **Cuadro General de Clasificación Archivística (CGCA):** Herramienta que identifica y organiza los tipos documentales producidos por cada unidad administrativa, agrupándolos en series documentales conforme a su función institucional; y,

2. **Catálogo de Disposición Documental (CDD):** Documento normativo que establece la vigencia documental, es decir, el tiempo que cada tipo de documento debe conservarse en archivo de trámite, concentración o histórico, así como el destino final de la información (eliminación o conservación permanente).

g) La **Matriz de Clasificación de Datos** consolida esta información, especificando para cada tipo de dato lo siguiente:

   1. El área responsable de su gestión;

   2. El tipo y nivel de confidencialidad de los datos;

   3. Los plazos mínimos y máximos de conservación en años;

   4. El formato, ya sea físico o digital; y,

   5. La acción final, tales como la transferencia, resguardo histórico o eliminación.

Este instrumento facilita a las unidades administrativas el cumplimiento de sus obligaciones en materia de conservación, depuración y disposición de la información, promoviendo la eficiencia operativa, la transparencia institucional y el cumplimiento normativo en protección de datos personales, archivos y rendición de cuentas.

IV. Responsabilidades

Para asegurar el cumplimiento efectivo de los plazos mínimos y máximos de conservación de datos, es esencial definir claramente las responsabilidades de los actores clave dentro de la SESEA:

a) **Dirección de Archivos:** Esta unidad es responsable de asesorar a las personas titulares de la información sobre los plazos adecuados para conservar los documentos, conforme a la normativa vigente. Además, supervisa que se cumplan correctamente los tiempos de retención y eliminación de datos documentales, garantizando la integridad y disponibilidad de la información archivada;

b) **Personal de Archivo:** Las personas servidoras públicas asignados a esta función son responsables de gestionar físicamente los archivos, velando por que se conserven y se eliminen conforme a la normativa aplicable y los instrumentos archivísticos correspondientes;

c) **Dirección de Normatividad y Asuntos Jurídicos:** Su función principal es interpretar y aplicar la legislación vigente relacionada con la conservación de datos. Proporciona asesoría legal en caso de dudas, conflictos o controversias que puedan surgir sobre el manejo y conservación de la información;

d) **Dirección de Servicios Tecnológicos y Plataforma Digital:** Está encargada de implementar y mantener los mecanismos técnicos necesarios para administrar los datos electrónicos, asegurando que se respeten los plazos de conservación establecidos. Esto incluye la eliminación segura o el archivado protegido de los datos digitales según corresponda; y,

e) **Todo el Personal:** Cada persona servidora pública de la SESEA tiene la responsabilidad de cumplir con esta política, gestionando y conservando los datos bajo su custodia de acuerdo con los plazos establecidos, contribuyendo así a una gestión documental ordenada y conforme a la ley.

CAPÍTULO IX
DE LA POLÍTICA DE CIFRADO DE DATOS

CIS CONTROL #3: PROTECCIÓN DE DATOS

I. **Propósito y Objetivo**

Establecer los lineamientos técnicos y operativos para garantizar el cifrado obligatorio de todos los dispositivos y sistemas que almacenan, procesan o transmiten información confidencial dentro de la SESEA. Asimismo, definir el procedimiento a seguir en caso de identificar equipos que no cumplan con esta medida de seguridad, con el fin de mitigar riesgos de acceso no autorizado, proteger la integridad y confidencialidad de los datos, y asegurar el cumplimiento de las disposiciones legales en materia de protección de información.

II. **Alcance**

Esta política aplica a todas las personas servidoras públicas, prestadores de servicios, contratistas y cualquier otro tercero que, en el ejercicio de sus funciones, utilice dispositivos o sistemas que almacenen, procesen o transmitan información institucional de carácter confidencial dentro de la SESEA. Incluye computadoras portátiles y de escritorio, servidores, dispositivos móviles, unidades de almacenamiento externas como USB, discos duros externos, así como plataformas en la nube utilizadas por la SESEA. La política abarca tanto el cifrado de datos en reposo como en tránsito, y establece los requerimientos mínimos que deben cumplir las herramientas y métodos de cifrado autorizados.

III. **Descripción de la política**

Para garantizar una protección efectiva, esta política exige el uso de algoritmos de cifrado reconocidos internacionalmente, como AES de 256 bits para datos en reposo y TLS 1.3 o superior para datos en tránsito, asegurando que la información esté resguardada durante todo su ciclo de vida.

Asimismo, se establece un marco estricto de gestión de claves criptográficas, que contempla la generación segura, almacenamiento protegido, preferentemente en HSM, rotación periódica y recuperación controlada de claves, de modo que solo

usuarios autorizados puedan acceder a los datos cifrados en situaciones justificadas.

Los dispositivos cifrados deberán incorporar mecanismos de autenticación multifactor (MFA), combinando al menos dos factores de autenticación que son el conocimiento, posesión o biometría, para prevenir accesos no autorizados, incluso en caso de pérdida o robo del equipo.

Se contemplan excepciones controladas al uso obligatorio del cifrado, permitidas únicamente bajo circunstancias excepcionales, y sujetas a la aprobación expresa de la Dirección de Servicios Tecnológicos. Tales casos deberán documentarse mediante oficio, incluir justificación técnica, responsable asignado, vigencia limitada, máximo 15 días naturales, y operar en entornos aislados sin conexión a redes ni acceso a información crítica.

Para facilitar el cumplimiento, se recomienda el uso de herramientas específicas según el sistema operativo o tipo de dispositivo, tales como:

a) BitLocker (Windows);

b) FileVault (macOS);

c) LUKS (Linux);

d) Cifrado nativo en dispositivos móviles (Android/iOS); y,

e) VeraCrypt o BitLocker To Go para medios extraíbles.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital es responsable de implementar, configurar y mantener los mecanismos de cifrado en los dispositivos institucionales que procesan o almacenan información confidencial. Asimismo, debe asegurar que estos sistemas cumplan con estándares técnicos reconocidos, brindar soporte técnico a las unidades usuarias, realizar auditorías periódicas para verificar el cumplimiento, y documentar cualquier excepción aprobada en los registros oficiales. Además, debe coordinar la respuesta ante detección de dispositivos sin

cifrado, gestionar la aplicación de medidas correctivas, y asegurar la trazabilidad de todo el proceso de regularización.

La Secretaría Técnica participa en la revisión y autorización de solicitudes excepcionales que impliquen el uso temporal de equipos no cifrados, evaluando su impacto y asegurando que se apliquen controles compensatorios que mitiguen riesgos operativos y de seguridad.

Por su parte, la Delegación Administrativa debe garantizar que todo equipo tecnológico adquirido cuente con capacidades de cifrado activadas o habilitadas desde su entrega. Asimismo, es responsable de validar que dichos equipos cumplan con las especificaciones técnicas requeridas y estén debidamente registrados en el inventario institucional antes de su asignación a usuarios finales.

Finalmente, los usuarios finales son responsables de mantener activos los mecanismos de cifrado en los dispositivos bajo su cargo, abstenerse de modificar o desactivar configuraciones de seguridad, y reportar de inmediato cualquier anomalía técnica o situación que comprometa la confidencialidad de la información institucional. Asimismo, deben colaborar con las áreas técnicas para facilitar auditorías o procesos de regularización en caso de incumplimiento.

V. **Procedimiento para Equipos sin Cifrado Detectados**

La detección de dispositivos no cifrados que manejan información confidencial constituye un incidente de seguridad que requiere respuesta inmediata y coordinada. El presente procedimiento establece las etapas secuenciales para la contención del riesgo, regularización técnica y formalización del cumplimiento, para garantizar que los equipos institucionales mantengan los estándares de protección requeridos.

Cuando se identifique un dispositivo que almacena información confidencial sin contar con cifrado activo, se ejecutará el protocolo de respuesta inmediata y regularización siguiente:

a) **Evaluación Integral del Riesgo:** La Dirección de Servicios Tecnológicos y Plataforma Digital llevará a cabo una evaluación exhaustiva para determinar el nivel de riesgo asociado al dispositivo detectado sin cifrado. Esta evaluación incluirá la verificación de la presencia de datos

confidenciales en el equipo, el análisis de su conexión a redes institucionales y otros sistemas críticos, la identificación de posible fuga de información, y la valoración del impacto potencial que la exposición podría generar. Con base en estos elementos, se clasificará la gravedad del incidente para definir y priorizar las medidas de contención y mitigación necesarias;

b) **Detección y Notificación Inmediata:** La Dirección de Servicios Tecnológicos y Plataforma Digital informará de manera inmediata al usuario responsable sobre el incumplimiento detectado, especificando la naturaleza de la vulnerabilidad identificada y los riesgos asociados. Simultáneamente, se registrará la detección en la bitácora de incidencias de seguridad (Anexo J), documentando fecha, hora, características del equipo, tipo de información expuesta y acciones preliminares adoptadas;

c) **Implementación de Medidas de Contención:** Se aplicarán controles temporales de seguridad que incluyen la restricción inmediata del acceso a la red institucional cuando se considere crítico, el bloqueo de funciones de sincronización automática y transferencia a medios extraíbles, y la marcación del equipo en el inventario técnico institucional, impidiendo su uso para actividades que involucren información sensible hasta su regularización completa;

d) **Proceso de Regularización Técnica:** La Dirección de Servicios Tecnológicos proporcionará asistencia técnica directa al usuario para la configuración e implementación del cifrado requerido, activando herramientas como BitLocker en entornos Windows o soluciones equivalentes según el sistema operativo. Este proceso incluye la verificación de la generación correcta de claves de recuperación, su almacenamiento seguro en repositorios autorizados, y la validación técnica del funcionamiento apropiado del cifrado implementado;

e) **Formalización y Actualización de Registros:** Al concluir exitosamente el proceso de cifrado, se actualizará el estado del equipo en el inventario técnico institucional (Anexo K). Asimismo, se solicitará al usuario que firme un documento en el que confirme haber recibido, comprendido y aceptado las políticas de seguridad vigentes, comprometiéndose a mantener activo el cifrado en el dispositivo y a reportar de manera

oportuna cualquier incidente o anomalía que pueda afectar la protección de la información; y,

f) **Protocolo para Casos de Reincidencia:** En situaciones donde el usuario o área presente incumplimientos recurrentes, se implementarán medidas progresivas que incluyen el bloqueo temporal del equipo hasta su adecuación definitiva, la realización de una revisión técnica exhaustiva y auditoría de seguridad del área involucrada, y la elaboración de un reporte detallado dirigido al Comité de Control Interno de la SESEA para la adopción de medidas administrativas correspondientes.

CAPÍTULO X
DE LA POLÍTICA PARA CONFIGURAR EQUIPOS DE COMPUTO

CIS CONTROL #4: MANTENER CONFIGURACIONES SEGURAS DOCUMENTADAS

I. Propósito y Objetivo

El propósito de esta política es establecer lineamientos claros para la configuración segura de equipos de cómputo, servidores, dispositivos móviles, aplicaciones, plataformas digitales, redes y Software utilizados en la SESEA. La intención es reducir los riesgos de seguridad informática, prevenir accesos no autorizados, mitigar vulnerabilidades técnicas y fortalecer la continuidad operativa de los servicios institucionales. Estos lineamientos buscan homogeneizar los criterios de seguridad, desde la instalación inicial hasta la operación cotidiana, bajo el marco de una gestión responsable y proactiva de los activos tecnológicos.

II. Alcance

La presente política aplica a todos los activos tecnológicos gestionados por la Dirección de Servicios Tecnológicos y Plataforma Digital. Esto incluye computadoras de escritorio, laptops, servidores físicos y virtuales, dispositivos móviles, dispositivos de red como switches, routers, puntos de acceso inalámbrico y firewalls, teléfonos IP y pantallas digitales asignadas para fines institucionales.

También se encuentran dentro del alcance los sistemas operativos, aplicaciones instaladas localmente, plataformas en la nube bajo administración directa, así como todo Software que se utilice en los equipos institucionales.

Quedan excluidos de esta política los dispositivos de videovigilancia u otros componentes clasificados como IoT que no se encuentren bajo la administración directa de la Dirección de Servicios Tecnológicos. No obstante, cualquier equipo conectado a la red institucional deberá observar principios básicos de seguridad y podrá ser sujeto a revisión técnica para evitar que represente un riesgo para la infraestructura tecnológica de la SESEA.

III. **Descripción de la Política**

Los equipos de cómputo constituyen el medio de acceso más común para acceder a información institucional, por ello, su configuración es fundamental, porque de esta manera, se protegen los datos que se generan en la SESEA, así como la integridad de la red institucional. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en dispositivos de cómputo siguiente:

a) **Actualizaciones del Sistema.** Activar actualizaciones automáticas del sistema operativo, Software antivirus y aplicaciones críticas, estableciendo ventanas de mantenimiento programadas para actualizaciones mayores que requieran reinicio;

b) **Gestión de Cuentas de Usuario.** Implementar el uso exclusivo de cuentas individuales para cada usuario, prohibiendo el uso de cuentas compartidas o genéricas. Los privilegios de administrador deben otorgarse únicamente cuando sean estrictamente necesarios y por tiempo limitado, aplicando el principio de menor privilegio. Cada cuenta debe contar con identificación única y trazabilidad completa de actividades;

c) **Políticas de contraseñas:** Aplicar políticas de uso de contraseñas únicas y requisitos de longitud, incluyendo la implementación de autenticación multifactor para cuentas administrativas y sistemas críticos. Las contraseñas deben cumplir con estándares de complejidad y deben ser renovadas según los intervalos establecidos institucionalmente;

d) **Cifrado de Información:** Activar obligatoriamente BitLocker o sistema de cifrado de disco completo aprobado por la Dirección de Servicios Tecnológicos, utilizando algoritmos de cifrado AES-256 como mínimo. Establecer procedimientos seguros para el resguardo y recuperación de claves de cifrado, incluyendo copias de seguridad cifradas almacenadas en ubicaciones físicamente separadas;

e) **Protección Antimalware:** Instalar solución antivirus con capacidades de detección y respuesta en punto final (EDR), conectada a consola de administración centralizada para monitoreo en tiempo real. La solución

debe incluir protección contra amenazas persistentes avanzadas, análisis de comportamiento y capacidades de respuesta automatizada ante incidentes;

f) **Firewall:** Mantener firewall local activado con configuración restrictiva por defecto, permitiendo únicamente el tráfico de red estrictamente necesario para las funciones laborales. Implementar reglas específicas para bloquear comunicaciones no autorizadas y registrar todos los intentos de conexión sospechosos;

g) **Control de Software:** Establecer lista blanca de aplicaciones aprobadas institucionalmente, e implementar tecnologías de control de aplicaciones que bloqueen la ejecución de Software no autorizado. Todos los programas deben ser validados por la Dirección de Servicios Tecnológicos antes de su implementación; y,

h) **Registro de actividad:** Activar registros de eventos de seguridad, accesos al sistema, cambios de configuración y actividades de usuario. Los logs deben ser enviados automáticamente a un sistema centralizado de gestión de eventos de seguridad, para análisis correlacionado y detección temprana de anomalías.

IV. Configuración Segura de Dispositivos Móviles

La naturaleza de los dispositivos móviles es su conectividad constante a diferentes sitios, este hecho los expone a riesgos como pérdida, robo, conexión a redes no seguras e instalación de aplicaciones maliciosas. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en dispositivos móviles siguiente:

a) **Autenticación de Dispositivo:** Establecer como obligatorio el uso de métodos de desbloqueo seguros, incluyendo PIN de mínimo 4-6 dígitos, patrón complejo, contraseña alfanumérica o biometría validada. Configuración de bloqueo automático después de máximo cinco minutos de inactividad, con un límite máximo de cinco intentos fallidos antes del borrado de datos;

b) **Cifrado Integral:** Activar cifrado completo del dispositivo utilizando estándares AES-256, incluyendo almacenamiento interno, tarjetas de memoria externa y aplicaciones de comunicación. Verificación que el cifrado está habilitado tanto en reposo como en tránsito para todas las comunicaciones institucionales;

c) **Gestión Móvil Empresarial:** Registrar obligatoriamente dicho dispositivo en el sistema de gestión móvil (MDM) institucional, para así poder administrarlo de manera remota;

d) **Actualización Sistemática:** Habilitar actualizaciones automáticas del sistema operativo y aplicaciones críticas, estableciendo políticas que requieran instalación de parches de seguridad dentro de los siete días posteriores a su disponibilidad. Mantener versiones mínimas aprobadas del sistema operativo;

e) **Control de Instalaciones:** Restringir instalaciones exclusivamente a tiendas oficiales de aplicaciones y catálogo institucional aprobado por la Dirección de Servicios Tecnológicos. Implementar filtros que bloqueen aplicaciones con permisos excesivos, origen dudoso o historial de vulnerabilidades de seguridad conocidas; y,

f) **Capacidades de Respuesta:** Configurar funcionalidades de borrado remoto completo, localización GPS, bloqueo remoto y envío de alertas automáticas en caso de pérdida, robo o compromiso del dispositivo. Establecer procedimientos de respuesta a incidentes específicos para dispositivos móviles.

V. Configuración Segura de Servidores

Los servidores representan el núcleo de la infraestructura tecnológica institucional, albergando aplicaciones, bases de datos y servicios esenciales para las actividades diarias. Alguna falla en estos puede resultar en interrupciones masivas de servicios, pérdida de información y daño a la imagen institucional. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en los servidores de la Secretaría siguiente:

a) **Principio de Servicios Mínimos:** Instalar exclusivamente los servicios y componentes estrictamente necesarios para la función específica del servidor, deshabilitando todos los servicios innecesarios. Realizar revisiones trimestrales para identificar y remover componentes no utilizados que puedan representar superficie de ataque adicional;

b) **Administración de Privilegios:** Implementar control de cuentas con privilegios administrativos, aplicando separación de funciones y el principio de menor privilegio. Establecer cuentas de servicio específicas con permisos mínimos necesarios y rotación periódica de credenciales administrativas cada 90 días;

c) **Cifrado y Protección de Datos:** Aplicar cifrado de discos completo en todos los servidores, incluyendo sistemas de archivos, bases de datos y respaldos. Implementar gestión segura de claves criptográficas con módulos de seguridad de hardware (HSM) cuando aplique, y procedimientos documentados para recuperación de claves;

d) **Acceso Remoto Seguro:** Establecer acceso remoto exclusivamente a través de VPN institucional con autenticación multifactor obligatoria, implementando controles de red basados en segmentación y principio de confianza cero. Deshabilitar protocolos inseguros como Telnet, FTP sin cifrar y RDP directo desde internet;

e) **Registro Integral de Eventos:** Habilitar logging comprehensivo de sistema, seguridad, auditoría, accesos y cambios de configuración, enviando logs a servidor centralizado con sincronización de tiempo NTP. Configurar alertas automáticas para eventos críticos de seguridad e intentos de acceso no autorizado; y,

f) **Monitoreo Continuo:** Integrar servidores con sistemas de monitoreo de infraestructura, alertas proactivas de rendimiento y seguridad, y herramientas de análisis de vulnerabilidades. Implementar monitoreo de integridad de archivos críticos del sistema y bases de datos.

VI. **Dispositivos IoT**

Los dispositivos del Internet de las Cosas (IoT) no están permitidos por las vulnerabilidades que suponen y la utilidad nula para los propósitos de la secretaría.

VII. **Configuración Segura de Sistemas Operativos**

El sistema operativo constituye la base fundamental sobre la cual funcionan todas las aplicaciones y servicios institucionales. Una configuración inadecuada del sistema operativo puede exponer vulnerabilidades que comprometan la seguridad integral del equipo, independientemente de las medidas de protección implementadas en capas superiores, haciendo crítica su configuración segura desde la instalación inicial. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en los sistemas operativos de la SESEA siguiente:

a) **Gestión de Versiones:** Utilizar exclusivamente versiones de sistemas operativos con soporte activo y extendido del fabricante, estableciendo un cronograma de migración antes del fin de soporte. Mantener inventario actualizado de versiones instaladas y planes de actualización documentados;

b) **Arranque Seguro:** Activar Secure Boot en todos los sistemas compatibles para verificar integridad del proceso de arranque y prevenir carga de código malicioso durante el inicio del sistema. Configurar TPM (Trusted Platform Module) cuando esté disponible para fortalecer la cadena de confianza;

c) **Minimización de Servicios:** Deshabilitar todos los servicios, protocolos y características innecesarias según el rol específico de cada equipo, aplicando plantillas de configuración basadas en marcos de referencia como CIS Controls. Documentar justificación para cada servicio habilitado;

d) **Políticas de Grupo Centralizadas:** Implementar y mantener políticas de grupo (GPO) centralizadas para control de acceso, configuración de pantalla de bloqueo, gestión de actualizaciones, restricciones de

Software y configuraciones de seguridad homogéneas en toda la infraestructura; y,

e) **Control de Interfaces:** Implementar restricciones apropiadas en puertos USB, Bluetooth, WiFi y otras interfaces según el nivel de riesgo del equipo y su ubicación. Establecer políticas que permitan únicamente dispositivos autorizados y registrados institucionalmente.

VIII. **Configuración Segura de Aplicaciones**

Las aplicaciones de Software procesan, almacenan y transmiten la información sensible de la SESEA, convirtiéndolas en objetivos principales para posibles atacantes. Configuraciones inseguras en aplicaciones pueden resultar en brechas de datos, accesos no autorizados y compromiso de procesos críticos de negocio, independientemente de la seguridad implementada en la infraestructura subyacente. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en la SESEA siguiente:

a) **Despliegue Centralizado:** Utilizar exclusivamente el catálogo de Software aprobado y validado, implementando distribución centralizada mediante herramientas de gestión de Software institucional. Establecer un proceso formal de evaluación y aprobación para nuevas aplicaciones;

b) **Configuración de Seguridad Específica:** Revisar y configurar políticas específicas de seguridad para cada aplicación, incluyendo gestión de contraseñas, configuración de sesiones, habilitación de logs de auditoría y controles de acceso basados en roles;

c) **Actualización Proactiva:** Mantener activadas las actualizaciones automáticas para plugins, dependencias, componentes y parches de seguridad. Establecer ventanas de mantenimiento programadas para actualizaciones que requieran interrupción de servicios;

d) **Integración con Monitoreo:** Configurar la integración de aplicaciones críticas con un sistema de monitoreo institucional para correlación de eventos, detección de anomalías y respuesta automatizada a incidentes

de seguridad. Implementar logging detallado de las actividades y transacciones de los usuarios; y,

e) **Verificación de Integridad:** Implementar verificación obligatoria de firmas digitales, checksums criptográficos y certificados de autenticidad previo a cualquier instalación o actualización de Software. Mantener una base de datos de hashes conocidos para Software aprobado.

IX. Gestión de Configuración de Control de Cambios

La gestión efectiva de configuraciones y el control riguroso de cambios son elementos fundamentales para mantener la postura de seguridad institucional a lo largo del tiempo. Sin procesos estructurados, las configuraciones seguras pueden degradarse inadvertidamente, creando ventanas de vulnerabilidad que comprometan la seguridad integral de la infraestructura tecnológica. Tomando esto en consideración, la Dirección de Servicios Tecnológicos ejecutará el protocolo de medidas de seguridad en la SESEA siguiente:

a) **Documentación de Configuraciones:** Mantener documentación detallada y actualizada de todas las configuraciones de seguridad implementadas, incluyendo justificación técnica, responsable de implementación y fecha de última revisión. Utilizar herramientas de gestión de configuración automatizadas cuando sea posible;

b) **Control de Cambios:** Implementar proceso formal de control de cambios para cualquier modificación a las configuraciones de seguridad, requiriendo aprobación previa, pruebas en ambiente no productivo y documentación de impacto. Mantener un registro histórico de todos los cambios realizados; y,

c) **Plantillas y Estándares:** Desarrollar y mantener plantillas de configuración segura para cada tipo de activo tecnológico, basadas en marcos de referencia internacionales como NIST, ISO 27001 y CIS Controls. Actualizar plantillas cuando surjan nuevas amenazas o recomendaciones.

X. **Normatividad de Referencia**

Esta política se alinea con las mejores prácticas de seguridad internacional definidas en los CIS Controls v8, particularmente en los siguientes controles críticos:

- **CIS Control 4:** Configuración Segura de Activos y Software Empresarial, que establece la necesidad de desarrollar y aplicar configuraciones seguras en todos los sistemas tecnológicos institucionales, incluyendo equipos de cómputo, servidores y dispositivos móviles;

- **CIS Control 5:** Administración de Cuentas, que establece buenas prácticas para el uso de cuentas individuales, privilegios mínimos y trazabilidad de accesos;

- **CIS Control 6:** Gestión de Control de Accesos, aplicable a la correcta asignación, monitoreo y revocación de privilegios;

- **CIS Control 7:** Gestión Continua de Vulnerabilidades, que sugiere el uso de parches, actualizaciones periódicas y evaluación del estado de los sistemas;

- **CIS Control 8:** Gestión de Registros de Auditoría, que establece lineamientos para el monitoreo de logs y generación de alertas;

- **CIS Control 10:** Defensas contra Malware, relacionado con la implementación de soluciones antimalware y mecanismos de protección en el punto final;

- **CIS Control 11:** Recuperación de Datos, en lo concerniente a respaldos y restauración de configuraciones seguras;

- **CIS Control 13:** Monitoreo y Defensa de la Red, específicamente en lo referente al uso de firewalls locales, segmentación y control del tráfico saliente;

- **CIS Control 16:** Seguridad en el Software de Aplicación, respecto a configuración segura, validación de integridad y control de dependencias; y,

- **CIS Control 17:** Gestión de Respuesta a Incidentes, que establece mecanismos para reaccionar ante configuraciones comprometidas o cambios no autorizados.

Además, se toman como referencia los estándares establecidos por la norma ISO/IEC 27001, específicamente en sus dominios de control de acceso, seguridad operativa y gestión de activos, así como las directrices complementarias detalladas en ISO/IEC 27002.

XI. **Responsabilidad**

La Dirección de Servicios Tecnológicos y Plataforma Digital es la instancia responsable de implementar, supervisar y mantener las configuraciones de seguridad descritas en esta política. A dicha Dirección corresponde asegurar que todos los activos bajo su administración cumplan con los lineamientos establecidos, así como coordinar las acciones necesarias para su aplicación efectiva y oportuna en colaboración con las áreas usuarias.

El personal técnico designado por la Dirección de Servicios Tecnológicos deberá ejecutar las configuraciones conforme a los protocolos vigentes, mantener actualizada la documentación correspondiente, registrar cambios de forma completa y proporcionar soporte ante incidentes relacionados con la configuración de activos.

Las personas usuarias, por su parte, están obligadas a respetar las configuraciones preestablecidas, abstenerse de realizar modificaciones sin autorización expresa y reportar cualquier anomalía, mal funcionamiento o señal de posible compromiso de los dispositivos asignados.

XII. **Respuesta a Incidentes de Configuración**

Incluso con las mejores medidas preventivas, pueden ocurrir incidentes relacionados con configuraciones de seguridad comprometidas, cambios no autorizados o errores de configuración. La capacidad de detectar, responder y recuperarse rápidamente de estos incidentes es crucial para minimizar el impacto operacional y mantener la continuidad de los servicios institucionales críticos. Tomando esto en consideración, la Dirección de Servicios Tecnológicos y

Plataforma Digital ejecutará el protocolo de medidas de seguridad en la SESEA siguiente:

a) **Detección y Respuesta:** Implementar sistemas de detección automatizada de cambios no autorizados en configuraciones, con alertas inmediatas al equipo de seguridad. Establecer procedimientos de respuesta que incluyan evaluación de impacto, contención, investigación y recomendación; y,

b) **Recuperación y Restauración:** Mantener respaldos seguros de configuraciones conocidamente buenas para permitir restauración rápida en caso de compromiso o error de configuración. Implementar puntos de restauración automatizados antes de cambios mayores.

CAPÍTULO XI
DE LA POLÍTICA PARA CONFIGURACIÓN DE DISPOSITIVOS DE RED

CIS CONTROL #4: MANTENER CONFIGURACIONES SEGURAS DOCUMENTADAS

I. Propósito y Objetivo

Los dispositivos de red son elementos críticos dentro de la infraestructura tecnológica de la SESEA. Su configuración y gestión adecuada son fundamentales para evitar interrupciones de servicios, accesos no autorizados y exposición de información confidencial. El propósito de esta política es establecer los lineamientos técnicos, que deben seguirse para configurar de manera segura todos los dispositivos de red, con el objetivo de proteger la infraestructura institucional contra riesgos como accesos no autorizados, ataques cibernéticos y configuraciones vulnerables.

II. Alcance

Esta política se aplica a todos los dispositivos de red de la SESEA, incluyendo dispositivos, y servicios de red, tanto internos como conexiones remotas. El cumplimiento de esta política es necesaria para asegurar que cada dispositivo de red esté configurado y administrado adecuadamente dentro de la infraestructura tecnológica institucional.

La configuración y el mantenimiento de los dispositivos de red serán gestionados principalmente por la Dirección de Servicios Tecnológicos. El objetivo de esta política es garantizar que todos los dispositivos de la red estén configurados y gestionados conforme con los protocolos de seguridad establecidos en esta política.

III. Descripción de la política

Todos los dispositivos de red deben ser configurados con un enfoque en la seguridad, adaptándose a las características y funciones específicas de cada tipo de dispositivo. Esto incluye la correcta configuración de firewalls para filtrar tráfico no autorizado, la segmentación de la red para reducir la exposición a dispositivos

sensibles y minimizar los riesgos de ataques cibernéticos, así como la implementación de contraseñas seguras.

Además, es esencial mantener una bitácora de auditoría detallada, que registre tanto las configuraciones iniciales como cualquier cambio o ajuste realizado a lo largo de su vida útil, garantizando el seguimiento y facilitando la detección de posibles irregularidades.

La seguridad de dispositivos de red depende de la implementación de procesos operativos estables. Es fundamental mantener configuraciones seguras a lo largo del tiempo y asegurarse de que cualquier cambio en la infraestructura se maneje adecuadamente. Para garantizar que el personal esté preparado para gestionar estos procesos, se deben seguir prácticas de capacitación continuas y actualización constante

IV. **Gestión de Cambios**

Los cambios en las configuraciones son críticas, porque se pueden introducir vulnerabilidades. Por ello, es esencial que la gestión de estos cambios se realice mediante procedimientos controlados. Esto incluye la capacitación constante del personal de la Dirección de Servicios Tecnológicos y Plataforma Digital para mejores prácticas para la administración de configuraciones seguras y en la importancia de seguir los pasos siguientes:

a) **Documentación:** Registrar cada cambio realizado, incluyendo el nombre de la persona responsable que realizó la configuración, fecha, descripción detallada, justificación y autorización en la Bitácora de Configuraciones Seguras;

b) **Respaldos:** Realizar un respaldo completo antes y después de cualquier modificación, lo que permitirá una restauración rápida (rollback) si es necesario; y,

c) **Revisiones:** Ejecutar revisiones periódicas (al menos semestrales) de configuraciones críticas, para verificar cumplimiento y efectividad de dichos procedimientos operativos.

V. **Gestión de Respaldos**

Los respaldos de configuración garantizan la continuidad operacional y permiten restauración rápida en caso de fallos o compromisos de seguridad. Para ello es fundamental implementar las medidas siguientes:

a) **Automatización:** Implementar respaldos automatizados; y,

b) **Almacenamiento:** Guardar respaldos cifrados en ubicación segura separada con control de acceso estricto.

VI. **Responsabilidades**

La configuración segura de dispositivos de red debe garantizar la protección de toda la infraestructura tecnológica institucional. Para lograrlo, se deben implementar las medidas de seguridad siguientes:

a) **Principio de Mínimo Privilegio:** El acceso a la configuración de dispositivos de red, se debe restringir exclusivamente al personal autorizado de la Dirección de Servicios Tecnológicos, utilizando cuentas individuales y un registro de actividades detallado;

b) **Reducción de Superficie de Ataque:** Se debe desactivar de manera obligatoria todos los servicios, protocolos y funcionalidades innecesarias para la operación específica de cada dispositivo, minimizando posibles ataques;

c) **Registro y Trazabilidad**: Toda modificación debe ser documentada en la Bitácora de Configuraciones Seguras (Anexo E) incluyendo el responsable, fecha, descripción del cambio y justificación del mismo, para garantizar la transparencia y facilitar la auditoría; y,

d) **Gestión Centralizada:** Los dispositivos deben permitir administración segura desde consolas protegidas utilizando protocolos cifrados y autenticación robusta, para asegurar un control adecuado.

VII. **Normatividad de referencia**

Esta política se fundamenta en las normativas tanto nacionales como internacionales, estas incluyen las normas ISO/IEC 27001 e ISO/IEC 27002, que abordan la gestión de la seguridad de información, así como la norma NIST SP 800-53, que proporciona controles para la protección de infraestructuras tecnológicas. En legislación nacional la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y la NOM 151.

CAPÍTULO XII
DE LA POLÍTICA PARA EL BLOQUEO AUTOMÁTICO DE DISPOSITIVOS

CIS CONTROL #4: MANTENER CONFIGURACIONES SEGURAS DOCUMENTADAS

I. Propósito y Objetivo

Establecer una medida de seguridad que garantice el bloqueo automático de dispositivos institucionales tras períodos de inactividad, con esta política tiene como objetivo reducir el riesgo de acceso no autorizado a información sensible, sistemas y recursos digitales, así como proteger la confidencialidad de datos institucionales cuando los dispositivos no estén siendo utilizados.

II. Alcance

Esta política aplica a todos los dispositivos y equipos tecnológicos utilizados por la SESEA, incluidos dispositivos internos como computadoras, servidores, entre otros, así como las conexiones remotas como VPN, acceso remoto a escritorios y servidores, y herramientas de administración remota como AnyDesk o TeamViewer. Abarca tanto la configuración y monitoreo de estos dispositivos, como la supervisión del personal responsable de su gestión. Su objetivo es garantizar la seguridad de la infraestructura tecnológica y proteger la información institucional contra accesos no autorizados y vulnerabilidades.

III. Descripción de la política

Esta política establece los lineamientos necesarios para garantizar la configuración segura y el monitoreo continuo de todos los dispositivos utilizados dentro de la SESEA. Abarca tanto los dispositivos internos, como computadoras y servidores, como las conexiones remotas, como las VPN y herramientas de administración remota.

Además, regula la supervisión del personal responsable de gestionar estos dispositivos, asegurando que se apliquen las mejores prácticas de seguridad en todo momento. La implementación de esta política tiene como objetivo fortalecer la protección de los recursos institucionales frente a amenazas cibernéticas y garantizar la continuidad operativa de los servicios tecnológicos esenciales.

IV. **Bloqueo por Tipo de Dispositivo**

La implementación del bloqueo automático debe ajustarse a las características específicas de cada tipo de dispositivo que pertenezca a la SESEA, considerando su función operativa y nivel de exposición a riesgos de seguridad. Los dispositivos se requieren una atención especial incluyen:

a) **Estaciones de Trabajo y Servidores**

Los equipos de cómputo, como laptops, servidores con interfaces gráficas y estaciones de trabajo con acceso libre, son puntos críticos que pueden exponer al sistema a vulnerabilidades. Por ello, se deben de aplicar las siguientes medidas:

Los equipos de cómputo, como laptops y servidores con interfaces gráficas, deben configurarse para activar automáticamente el bloqueo de pantalla después de un tiempo máximo de inactividad de 15 minutos (900 segundos), requiriendo autenticación para reanudar la sesión. Además, se debe habilitar un protector de pantalla con contraseña obligatoria al reanudar la actividad, y garantizar que el tiempo de inactividad no supere los 900 segundos, sin excepciones.

Esta configuración debe ser gestionada mediante políticas de grupo centralizadas, siempre que sea técnicamente factible, y se debe deshabilitar la capacidad de los usuarios finales para modificar estos parámetros. En el caso de los servidores que utilicen interfaces gráficas, se debe aplicar la misma política de bloqueo automático, configurando el bloqueo de forma independiente para cada sesión administrativa concurrente. Además, se deberá documentar cualquier excepción que permita sesiones extendidas para procesos críticos que lo requieran.

b) **Dispositivos Móviles**

Los dispositivos móviles presentan un mayor riesgo de pérdida o robo, por lo que requieren medidas de seguridad más estrictas. Es indispensable configurar el bloqueo automático de pantalla tras dos minutos (120 segundos) de inactividad, requiriendo autenticación para el acceso posterior. Además, se debe exigir un PIN de al menos seis dígitos, una contraseña alfanumérica

robusta, autenticación validada o un patrón de desbloqueo complejo, prohibiendo métodos inseguros como deslizar la pantalla sin autenticación o configuraciones sin ningún tipo de seguridad.

La gestión de los dispositivos debe realizarse de manera centralizada a través de plataformas de Mobile Device Management (MDM) para dispositivos corporativos, aplicando políticas de Exchange ActiveSync para aquellos con acceso al correo institucional y estableciendo políticas de cumplimiento (compliance) para garantizar que solo los dispositivos que cumplan con estos requisitos puedan acceder a los recursos institucionales.

La efectividad de los controles de bloqueo depende de su implementación y mantenimiento a través de herramientas de gestión centralizadas, por ello es indispensable tener en cuenta:

1. **Métodos de Implementación:**

   1.1. Implementación Automatizada: Utilizar políticas de grupo (GPO) para entornos Windows, herramientas de configuración centralizada para sistemas Linux, plataformas de bloqueo para dispositivos móviles, y scripts de configuración automatizados cuando sea aplicable;

   1.2. Configuración Manual: En casos donde la gestión centralizada no sea factible, implementar configuraciones manuales siguiendo procedimientos documentados, verificar dicha implementación mediante checklist de validación, y programar revisiones periódicas de cumplimiento; y,

   1.3. Validación de Configuración: Ejecutar pruebas de funcionamiento después de la implementación, verificar tiempos de bloqueo configurados mediante medición cronometrada, y confirmar que usuarios no puedan modificar configuraciones establecidas.

V. **Monitoreo y Mantenimiento:**

a) **Auditorías:** La Dirección de Servicios Tecnológicos ejecutará auditorías trimestrales para revisar el cumplimiento de configuraciones, identificar dispositivos que no cumplan con políticas establecidas, y generar reportes de cumplimiento para seguimiento gerencial;

b) **Corrección:** Solicitar correcciones inmediatas cuando se identifiquen dispositivos no conformes, establecer plazo máximo de 48 horas para remediar incumplimientos, y documentar acciones correctivas;

c) **Gestión de Excepciones:** Las excepciones a esta política se evaluarán caso por caso, tomando en cuenta los riesgos de seguridad necesarios. Las solicitudes de excepción deben ser aprobadas por la Dirección de Servicios Tecnológicos y documentadas en la Bitácora de Relación y Análisis de Equipos (Anexo F). Las excepciones se revisarán cada seis meses para asegurar que los controles de seguridad sigan siendo efectivos; y,

d) **Cumplimiento y Consecuencias:** El cumplimiento de esta política es obligatorio y su incumplimiento puede generar medidas disciplinarias. El personal de la SESEA debe reportar los fallos en los dispositivos y actualizaciones, no modificar configuraciones sin autorización y mantener credenciales seguras. La Dirección de Servicios Tecnológicos será responsable de implementar las configuraciones adecuadas, monitorear el cumplimiento.

VI. **Responsabilidades**

La Dirección de Servicios Tecnológicos es responsable de implementar y gestionar esta política de bloqueo automático, para todos los dispositivos utilizados por la SESEA. Esto incluye asegurar que todos los equipos sean configurados para que después de un periodo de inactividad determinado, se bloqueen automáticamente con el fin de prevenir accesos no autorizados. Además, la Dirección de Servicios Tecnológicos debe de supervisar de manera continua el cumplimiento de esta política y realizar auditorías periódicas para garantizar su correcta implementación.

En caso de ser necesario, la Dirección de Servicios Tecnológicos proporcionará alguna capacitación al personal para asegurar el correcto funcionamiento de estas medidas y actualizar los dispositivos de vulnerabilidades de seguridad, que puedan afectar este mecanismo de protección.

Dentro de sus funciones, la Dirección de Servicios Tecnológicos también tiene como objetivo configurar correctamente los parámetros de bloqueo automático, de acuerdo con esta política, además de registrar cualquier cambio realizado en la Bitácora de Configuraciones Seguras y realizar el seguimiento de los ajustes aplicados.

Por su parte, el personal de la SESEA es responsable de cumplir con esta política utilizando contraseñas seguras y asegurándose de que sus dispositivos estén configurados para bloquearse automáticamente después de un período de inactividad. Los usuarios no deben realizar modificaciones en la configuración del bloqueo automático sin la debida autorización de la Dirección de Servicios Tecnológicos, y deben asegurarse de que sus dispositivos se bloqueen adecuadamente cuando no estén en uso para evitar accesos no autorizados.

CAPÍTULO XIII
DE LA POLÍTICA PARA CONFIGURAR LA INFRAESTRUCTURA DE RED

CIS CONTROL #4: MANTENER CONFIGURACIONES SEGURAS DOCUMENTADAS

I. Propósito y Objetivo

Establecer lineamientos que garanticen el uso exclusivo de protocolos y configuraciones seguras para todo el acceso administrativo a servidores, dispositivos de red, sistemas operativos y plataformas tecnológicas institucionales. Esta política tiene como objetivo proteger la confidencialidad, integridad y autenticidad de las comunicaciones administrativas, asegurando la protección de la infraestructura de red contra interceptación, manipulación y accesos no autorizados.

II. Alcance

Esta política aplica a todos los servidores, dispositivos de red, sistemas operativos y plataformas tecnológicas de la SESEA que requieran acceso administrativo. Incluye tanto dispositivos internos como son servidores, estaciones de trabajo y equipos de red como conexiones remotas tales como VPN, acceso remoto, herramientas de administración remota. Excluye equipos personales y dispositivos no utilizados en funciones administrativas.

III. Descripción de la política

Esta política establece los lineamientos para garantizar el uso exclusivo de los protocolos y configuraciones seguras de acceso administrativo a los recursos tecnológicos de la SESEA. Incluye la implementación de mecanismos de autenticación robusta y el uso adecuado de protocolos para asegurar que las comunicaciones administrativas sean confidenciales, íntegras y auténticas. De esta manera se minimizan los riesgos de intercepción, manipulación y acceso no autorizado.

La selección de los protocolos para administración remota se basa en estándares de seguridad que proporcionan cifrado robusto, autenticación confiable y protección contra ataques de interceptación. Esta política establece las directrices para los

protocolos de comunicación aceptados y los que están expresamente prohibidos, asegurando así la integridad y la seguridad de la infraestructura tecnológica de la SESEA.

Tipo de protocolo	Protocolos Aceptados	Protocolos No Aceptados
Acceso Administrativo	SSH (versión 2 o superior) para acceso remoto a sistemas Unix, Linux y equipos de red.	Telnet (transmisión de datos en texto plano).
	RDP (Remote Desktop Protocol) con cifrado TLS habilitado y autenticación a nivel de red.	HTTP sin cifrado (para interfaces administrativas web, transferencia de archivos, etc.).
Interfaces Web	HTTPS con TLS 1.2 o superior, validando certificados SSL/TLS y configurando cipher suites seguras.	FTP sin cifrado (puerto 21).
Transferencia de archivos	-SFTP (SSH File Transfer Protocol), SCP (Secure Copy Protocol), FTPS (FTP over SSL/TLS).	R-Commands (rlogin, rsh, rexec, etc.).
API y Comunicaciones	HTTPS con autenticación robusta (tokens, certificados o OAuth 2.0).	SNMPv1 y SNMPv2c (sin autenticación ni cifrado).
Servicios Expuestos	Uso de servicios administrativos solo con protección VPN o túneles seguros intermedios.	Exponer servicios administrativos directamente en puertos abiertos al público sin protección.

Para la implementación de esta política se debe tener la configuración por defecto siguiente:

a) **Nuevos Sistemas:** La Dirección de Servicios Tecnológicos debe asegurar que todos los equipos y servidores nuevos se configuren con protocolos seguros habilitados por defecto y protocolos inseguros completamente deshabitados antes de puesta en producción;

b) **Plantillas de Configuración:** Desarrollar y mantener plantillas de configuración segura para diferentes tipos de sistemas incluyendo

servidores Windows y Linux, dispositivos de red y plataformas especializadas; y,

c) **Proceso de Despliegue:** Establecer checklist de verificación que confirme configuración de protocolos seguros antes de autorizar operación de nuevos sistemas en la red de producción.

IV. **Medidas de Seguridad Adicionales**

Complementar los controles de protocolo con medidas de protección en profundidad que fortalezcan la seguridad integral de accesos administrativos, entre ellas se encuentra:

a) **Autenticación Basada en Claves**: Priorizar el uso de claves SSH criptográficas o certificados digitales sobre autenticación por contraseña para accesos administrativos críticos. Implementar gestión centralizada de claves con rotación periódica;

b) **Autenticación Multifactor:** Implementar MFA para todos los accesos administrativos cuando sea técnicamente soportado por la plataforma, incluyendo tokens de hardware, aplicaciones de autenticación móvil o certificados digitales;

c) **Túneles VPN:** Utilizar conexiones VPN institucionales como capa adicional de protección para accesos administrativos desde ubicaciones remotas o redes no controladas;

d) **Mantenimiento de Servicios:** Mantener actualizados todos los servicios que proporcionan acceso administrativo, incluyendo OpenSSH, servidores web, servicios RDP y plataformas de gestión, aplicando parches de seguridad dentro de los 30 días posteriores a su disponibilidad;

e) **Redes Administrativas:** Implementar segmentación de red que aísle tráfico administrativo en VLANs o subredes dedicadas con políticas de firewall restrictivas; y,

f) **Estaciones de Administración:** Designar estaciones de trabajo específicas para actividades administrativas con configuraciones de seguridad endurecidas y acceso controlado a herramientas de administración.

V. Responsabilidades

La Dirección de Servicios Tecnológicos y Plataforma Digital es responsable de implementar, gestionar y mantener las configuraciones de acceso administrativo seguro en toda la infraestructura tecnológica de la SESEA. Esto incluye garantizar que todos los accesos a servidores, dispositivos de red, sistemas operativos y plataformas tecnológicas institucionales se realicen mediante protocolos seguros, además se debe de estar monitoreando continuamente el cumplimiento de esta política, realizando auditorías periódicas y ajustes cuando sea necesario.

CAPÍTULO XIV
DE LA POLÍTICA PARA LA ADMINISTRACIÓN DE CUENTAS PREDETERMINADAS DE LOS DISPOSITIVOS TECNOLÓGICOS

CIS CONTROL #4: MANTENER CONFIGURACIONES SEGURAS DOCUMENTADAS

I. **Propósito y Objetivo**

Esta política tiene como objetivo establecer los lineamientos obligatorios para la gestión de cuentas predeterminadas en todos los dispositivos de la SESEA, su finalidad es prevenir accesos no autorizados, reducir riesgos y eliminar vulnerabilidades asociadas con configuraciones y cuentas creadas con fines de prueba en los diferentes sistemas.

II. **Alcance**

Esta política aplica a todos los dispositivos tecnológicos de la SESEA, incluyendo servidores, equipos de red, dispositivos móviles, estaciones de trabajo y sistemas operativos. Se enfoca en las cuentas predeterminadas creadas durante la instalación, configuración inicial o pruebas de los dispositivos, ya sean propiedad de la SESEA o gestionados por personal administrativo. Todo el personal encargado de la administración, configuración y mantenimiento de estos dispositivos debe cumplir con esta política para garantizar la seguridad operativa, minimizando riesgos y vulnerabilidades causadas por cuentas predeterminadas no actualizadas o mal configuradas.

III. **Descripción de la política**

Esta política establece los lineamientos para gestionar las cuentas predeterminadas en los dispositivos tecnológicos de la SESEA. Su objetivo es prevenir accesos no autorizados y reducir riesgos de seguridad eliminando o modificando las cuentas predeterminadas creadas durante la instalación o configuración inicial. Se requiere deshabilitar, modificar contraseñas predeterminadas y documentar cada cambio para garantizar la protección adecuada tanto de los sistemas como de los dispositivos de la SESEA.

Se consideran cuentas predeterminadas todas aquellas que cuentan con credenciales de acceso, creadas automáticamente por fabricantes de hardware, desarrolladores de Software o sistemas operativos durante procesos de instalación inicial, configuración de fábrica o despliegue por defecto, incluyendo, pero no limitándose a credenciales con nombres estándar de la industria.

Toda cuenta predeterminada deberá ser evaluada técnicamente después de su instalación. Dependiendo de su función, se tomarán las acciones siguientes:

a) **Deshabilitación Controlada:** Si la cuenta no es esencial para el funcionamiento, se deshabilitará usando comandos administrativos;

b) **Eliminación Definitiva:** Si la cuenta no es crítica, se eliminará después de verificar dependencias en entornos de desarrollo o pruebas, asegurando que no afecte servicios clave;

c) **Renombramiento Estratégico:** Si no se puede deshabilitar o eliminar, se renombrará la cuenta de manera que no revele su propósito ni facilite ataques; y,

d) **Fortalecimiento de Credenciales:** Si la cuenta debe mantenerse activa, su contraseña será cambiada inmediatamente por una más robusta, siguiendo los estándares de seguridad establecidos.

IV. Responsabilidades

El personal de la Dirección de Servicios Tecnológicos tiene la responsabilidad de identificar, modificar o eliminar las cuentas predeterminadas en los dispositivos tecnológicos de la SESEA. Esto implica cambiar las contraseñas por defecto, desactivar cuentas innecesarias y documentar todos los cambios realizados. Además, deben realizar auditorías periódicas para asegurar que se cumpla con esta política y prevenir posibles vulnerabilidades.

V. Normativa de referencia

La normativa de referencia para la gestión de cuentas predeterminadas se basa en ISO/IEC 27001, ISO/IEC 27002, que proporcionan directrices sobre seguridad de la información, control de acceso y gestión de riesgos. Estas normas aseguran la

correcta administración, deshabilitación o fortalecimiento de cuentas predeterminadas en sistemas tecnológicos, alineándose con las mejores prácticas en Ciberseguridad.

CAPÍTULO XV
DE LA POLÍTICA PARA LA GESTIÓN DE CUENTAS DE USUARIO

CIS CONTROL #5: ADMINISTRACIÓN DE CUENTAS

I. Propósito y Objetivo

En la presente política se establece el marco normativo y procedimental para la gestión integral del ciclo de vida de cuentas de usuario general y usuario administrador, y su acceso a todos los sistemas y plataformas digitales de la SESEA. Con esta política se busca garantizar el control de accesos, la trazabilidad completa de operaciones y la conformidad con estándares de seguridad de la información aplicables a instituciones gubernamentales.

II. Alcance

Esta política aplica a todas las cuentas de usuario que requieran acceso a sistemas y plataformas digitales de la SESEA, incluyendo tanto cuentas de usuario general como cuentas con privilegios administrativos. El alcance comprende el ciclo de vida completo de las cuentas desde su creación hasta su eliminación, abarcando los procesos de solicitud, validación, implementación, modificación y desactivación.

La política se extiende a todos los colaboradores de la SESEA, incluyendo personal de estructura y por honorarios que requieran acceso a recursos tecnológicos institucionales. También incluye los sistemas de gestión de identidades, plataformas, aplicaciones y cualquier sistema que maneje autenticación y autorización de usuarios dentro del ecosistema tecnológico de la SESEA.

III. Descripción de la política

El proceso para crear cuentas de usuario depende de las funciones y atribuciones de dicho usuario en la SESEA. Esto porque en dicha Secretaría, se pueden crear dos cuentas diferentes usuarios; usuario general y usuario administrador. En ambos casos se debe seguir un procedimiento base para su creación, la única diferencia corresponde a la cantidad de permisos.

En este proceso se debe tomar en consideración las etapas siguientes:

a) **Iniciación del Proceso:** Todo requerimiento de creación de cuenta debe iniciarse mediante solicitud formal presentada por el responsable, a través de oficio dirigido a la Dirección de Servicios Tecnológicos y Plataforma Digital. Esta solicitud debe incluir identificación completa del usuario solicitante, puesto desempeñado según organigrama oficial, área de adscripción, justificación de necesidad de acceso basada en funciones laborales, sistemas o aplicaciones específicas requeridas, nivel de privilegios solicitado con justificación técnica, supervisor directo responsable de autorizar el acceso, y fecha estimada de inicio de necesidad;

b) **Proceso de Validación:** La Dirección de Servicios Tecnológicos debe ejecutar un proceso de validación que incluya verificación de la identidad del solicitante, confirmación de la vigencia de la relación laboral y del puesto desempeñado, validación de la necesidad técnica del acceso solicitado mediante análisis de funciones laborales, verificación de que no existen cuentas duplicadas o previamente asignadas al mismo usuario, y confirmación de autorización del supervisor directo mediante comunicación directa;

c) **Implementación:** Una vez completada la validación, la Dirección de Servicios Tecnológicos debe procederse a la creación de la cuenta siguiendo los estándares técnicos específicos que incluyan nomenclatura estandarizada basada en nombre y apellido del usuario; asignación al grupo de seguridad apropiado según el rol laboral definido; configuración de contraseña temporal robusta; habilitación de la obligación de cambio de contraseña en el primer inicio de sesión, y configuración de políticas de seguridad específicas del grupo asignado;

d) **Entrega Segura de Credenciales:** Las credenciales deben ser entregadas exclusivamente al usuario autorizado mediante proceso que garantice confidencialidad, incluyendo entrega presencial con verificación de identidad mediante identificación oficial, uso de sobre sellado para credenciales temporales, instrucciones específicas sobre cambio obligatorio de contraseña, orientación sobre políticas de seguridad aplicables, y confirmación de recepción mediante acuse firmado que se incorpore al expediente del usuario.

Además de estos, para la creación de cuentas del tipo administrador se debe tomar en consideración lo siguiente:

a) **Requisitos Adicionales:** Las cuentas con privilegios administrativos requieren un proceso de aprobación que incluya justificación detallada, donde se explique la necesidad específica de privilegios elevados, análisis de riesgos asociados con la asignación de privilegios administrativos, definición clara del alcance temporal de los privilegios requeridos, identificación de sistemas específicos donde se ejercerán privilegios administrativos, y aprobación explícita de la Dirección de Servicios Tecnológicos mediante documento firmado;

b) **Configuración Técnica Especializada:** Las cuentas administrativas deben ser creadas bajo esquemas de seguridad reforzados que incluyan nomenclatura donde se identifique claramente el carácter administrativo. Implementar obligatoriamente autenticación multifactor utilizando tokens de hardware o aplicaciones móviles certificadas. Poseer configuración de políticas de contraseñas más restrictivas, cuya longitud mínima corresponde de 8-16 caracteres y renovación cada 60 días. Habilitación de registro detallado de todas las actividades administrativas en logs centralizados. Configuración de alertas automáticas para actividades de alto riesgo; y,

c) **Principio de Cuentas Nominales:** Está estrictamente prohibido el uso compartido de cuentas administrativas, se debe asignar una cuenta única e individual a cada administrador autorizado. Esta cuenta debe ser claramente trazable al usuario responsable y debe mantener un registro detallado de todas las actividades realizadas para efectos de auditoría y rendición de cuentas.

En caso de ser necesario realizar modificaciones a cuentas existentes, se debe seguir un proceso que asegure la trazabilidad y el control de cambios. Entre las modificaciones permitidas se pueden incluir cambios en nombres de usuario, actualizaciones de información personal, modificaciones en asignación de grupos de seguridad, cambios en direcciones de correo electrónico asociadas, actualizaciones en información de contacto, y modificaciones en configuraciones de seguridad, para ello se debe seguir el proceso siguiente:

a) **Solicitud.** Toda solicitud de modificación debe ser presentada por escrito por el responsable, y ser enviada a la Dirección de Servicios Tecnológicos y Plataforma Digital, especificando claramente la naturaleza exacta de la modificación solicitada, justificación que respalde la necesidad del cambio, impacto esperado en las funciones laborales del usuario, sistemas que serán afectados por la modificación, y autorización del supervisor directo mediante firma en la solicitud

b) **Evaluación de Impacto.** Antes de implementar cualquier modificación, se debe ejecutar una evaluación de impacto por parte de la Dirección de Servicios Tecnológicos donde se analicen las implicaciones de seguridad del cambio propuesto, se identifique posibles conflictos con políticas de seguridad vigentes, se determine si la modificación requiere aprobaciones adicionales, se evalúen daños colaterales en usuarios o sistemas, y se establezca un plan de reversión en caso de problemas; y,

c) **Implementación y Documentación.** Las modificaciones deben ser realizadas exclusivamente por personal de la Dirección de Servicios Tecnológicos, registrando la fecha y hora de implementación, responsable técnico que ejecutó el cambio, detalles específicos de la modificación realizada, resultados de pruebas de funcionamiento post-modificación, y notificación al usuario afectado cuando sea aplicable.

Cuando un usuario experimente cambios en sus funciones laborales, promociones, transferencias entre áreas o modificaciones en responsabilidades, las modificaciones de datos deben ejecutarse inmediatamente para asegurar la alineación del usuario con las nuevas funciones. Este proceso debe completarse dentro de las 48 horas posteriores a la notificación oficial del cambio organizacional.

En el supuesto que un usuario termine la relación de trabajo con la SESEA, se debe eliminar su cuenta de usuario, con base en el proceso siguiente:

a) **Notificación y Coordinación:** El Departamento de Recursos Humanos, Financieros y Materiales o la Delegación Administrativa debe notificar formalmente a la Dirección de Servicios Tecnológicos sobre la desvinculación de cualquier colaborador inmediatamente. Esta notificación debe incluir identificación completa del usuario, fecha

efectiva de terminación, tipo de desvinculación (renuncia, despido, jubilación, entre otros.), necesidad de preservación de información específica, y responsable autorizado para recibir transferencia de datos críticos;

b) **Desactivación Inmediata:** Dentro de un plazo máximo de 24 horas posteriores a la notificación oficial, la Dirección de Servicios Tecnológicos debe ejecutar la desactivación completa de todas las cuentas asociadas al usuario desvinculado de los sistemas y plataformas de la SESEA; y,

c) **Preservación y Transferencia de Datos:** Cuando sea necesario preservar información crítica o transferir responsabilidades, debe ejecutarse un proceso controlado que incluya identificación de datos críticos que requieren preservación, transferencia de propiedad de archivos, backup de información según requerimientos del área, y documentación detallada de todos los datos transferidos para efectos de auditoría.

IV. Buenas prácticas y controles adicionales

Todo otorgamiento de cuentas de usuario debe basarse en un análisis detallado de las funciones laborales específicas de dicho usuario, asignando únicamente los accesos necesarios para el desempeño efectivo de sus responsabilidades. Para crear y asignar se deben seguir las recomendaciones siguientes:

a) Las cuentas de usuario deben seguir una nomenclatura estandarizada que facilite la identificación y gestión. Esta nomenclatura debe ser consistente en todos los sistemas y aplicaciones institucionales;

b) Las cuentas con privilegios administrativos deben identificarse claramente mediante el prefijo "adm." seguido de la nomenclatura del usuario, facilitando su identificación en logs de auditoría y sistemas de monitoreo. Está prohibido el uso de nombres genéricos como "admin", "administrator" o "root" para cuentas operativas; y,

c) Todas las cuentas con privilegios administrativos deben implementar obligatoriamente autenticación multifactor utilizando tokens de hardware compatibles con estándares FIDO2 o aplicaciones móviles de

autenticación basadas en algoritmos TOTP. Las cuentas de usuario regular que accedan a sistemas críticos o información sensible también deben implementar este control adicional.

Para actividades administrativas se debe implementar un modelo de escalamiento temporal que requiera autenticación adicional para obtener privilegios elevados por períodos limitados.

V. **Responsabilidades**

a) **Dirección de Servicios Tecnológicos y Plataforma Digital:** Responsable de la implementación técnica de todos los procesos de gestión de cuentas, incluyendo la validación de solicitudes, creación y configuración de cuentas según estándares establecidos, y mantenimiento de la infraestructura de autenticación. Debe ejecutar las auditorías internas trimestrales, mantener la documentación actualizada de todos los procedimientos y garantizar el cumplimiento de las políticas de seguridad en la gestión de identidades y accesos;

b) **Delegación Administrativa:** Unidad encargada de notificar formalmente a la Dirección de Servicios Tecnológicos sobre altas, bajas y modificaciones en la situación laboral del personal dentro de los plazos establecidos. Debe validar la información laboral de los solicitantes y coordinar con la Dirección de Servicios Tecnológicos para asegurar que los accesos se alineen con las funciones organizacionales de cada usuario;

c) **Titulares de las unidades de la SESEA:** Responsables de autorizar las solicitudes de acceso de su personal subordinado, validando que los privilegios solicitados correspondan efectivamente a las funciones laborales asignadas. Deben notificar inmediatamente cualquier cambio en las responsabilidades de sus colaboradores que pueda impactar en los requerimientos de acceso.

En el supuesto que, por recursos tecnológicos insuficientes, sea necesario que dos o más integrantes de cada unidad administrativa de la SESEA tengan el acceso compartido a través de la misma cuenta, será

obligación de la persona titular de dicha unidad informar a la Dirección de Servicios Tecnológicos acerca de las personas servidoras públicas que tienen el acceso compartido. Como parte de la información que deben entregar es el nombre de las personas servidoras públicas, puesto y equipo de cómputo por el cual tienen acceso. Es importante notificar de manera inmediata cuando esto ocurra, porque en todos los equipos de cómputo y servidores se guarda registro de las actividades, y en el supuesto de detectar actividades inusuales, la Dirección de Servicios Tecnológicos van a tomar las medidas necesarias para mitigar tal efecto, esto con base a los lineamientos de contingencia aprobados en el 2021; y,

d) **Usuarios Finales:** Encargados de presentar las solicitudes formales de creación de sus cuentas mediante oficio dirigido a la Dirección de Servicios Tecnológicos, incluyendo toda la información requerida y la justificación técnica correspondiente. Deben coordinar con el Departamento de Recursos Humanos, Financieros y Materiales para asegurar la coherencia entre los requerimientos de acceso y la estructura organizacional.

También son obligados a cumplir con las políticas de seguridad establecidas, incluyendo el cambio obligatorio de contraseñas temporales, el uso adecuado de sus credenciales y la notificación inmediata de cualquier incidente de seguridad. Deben colaborar en los procesos de auditoría y revisión periódica de accesos.

CAPÍTULO XVI
DE LA POLÍTICA PARA EL USO DE CONTRASEÑAS

CIS CONTROL #5: ADMINISTRACIÓN DE CUENTAS

I. **Propósito y Objetivo**

En la presente política se establece el marco normativo y procedimental para la gestión de contraseñas en todos los activos tecnológicos y cuentas institucionales de la SESEA, garantizando así la protección de la integridad, confidencialidad y disponibilidad de los sistemas de información mediante la implementación de credenciales seguras y únicas.

II. **Alcance**

Esta política aplica a todos los usuarios que tengan acceso a los sistemas de información de la SESEA. El alcance incluye todas las cuentas institucionales, sistemas operativos, aplicaciones, plataformas web, servicios en la nube y dispositivos tecnológicos que requieren autenticación mediante credenciales de acceso.

La política abarca tanto cuentas de usuario estándar como cuentas administrativas y de alto privilegio, independientemente de si utilizan autenticación multifactor o no. Se incluyen también las cuentas de servicio, cuentas compartidas institucionales y cualquier sistema que maneje información sensible o crítica de la organización. Esta cobertura se extiende a todos los entornos tecnológicos, desde infraestructura local hasta servicios externos contratados que requieran credenciales institucionales.

III. **Descripción de la política**

El proceso para crear contraseñas independientes del tipo de sistema, plataforma o aplicación para la cual se está creando, así como usuario involucrado debe estar homologado y ser seguro. Además de estas características, la contraseña a generar o modificar debe estar sujeta a una longitud y a una complejidad mínima que se debe de cubrir. Para generar/modificar contraseñas en la Dirección de Servicios Tecnológicos y Plataforma Digital se deben seguir las restricciones siguientes:

a) Toda cuenta institucional debe poseer una contraseña única y exclusiva que no se reutilice entre diferentes plataformas, sistemas o dispositivos. Esta unicidad debe mantenerse para evitar ataques cibernéticos;

b) Está prohibido compartir contraseñas entre usuarios, independientemente del nivel jerárquico o la naturaleza de la colaboración laboral. Cada usuario debe mantener la confidencialidad absoluta de sus credenciales y asumir responsabilidad total por las actividades realizadas con sus cuentas de acceso; y,

c) Las contraseñas se deben almacenar exclusivamente en gestores de contraseñas certificados o sistemas de autenticación institucionales con cifrado robusto. Está prohibido el almacenamiento en documentos físicos sin protección, archivos digitales sin cifrado, notas adhesivas, o cualquier medio que pueda ser accedido por terceros no autorizados.

Los requisitos de longitud de contraseñas fueron establecidos de acuerdo a un enfoque basado en riesgos, y un generador de autentificación multifactor, con los cuales se equilibra la seguridad y usabilidad operacional, dando como resultado las configuraciones de cuentas siguientes:

a) **Cuentas de Usuario con Autenticación Multifactor.** Las cuentas MFA requieren contraseñas de mínimo ocho caracteres, dado que proporcionan un segundo factor de autenticación para compensar la longitud reducida;

b) **Cuentas de Usuario sin Autenticación Multifactor.** Las cuentas sin MFA deben tener contraseñas de mínimo 14 caracteres para compensar la ausencia del factor adicional de seguridad; y,

c) **Cuentas Administrativas y de Alto Privilegio.** Todas las cuentas con privilegios de administrador deben tener longitud mínima de 14 caracteres, independientemente del uso de MFA, con implementación altamente recomendada de autenticación multifactor como control de seguridad adicional.

Los tipos de caracteres empleados en las contraseñas deben estar sujetos a:

a) **Elementos Recomendados**. Las contraseñas deben incorporar una diversidad de caracteres incluyendo letras mayúsculas y minúsculas para incrementar el espacio de claves posibles, dígitos numéricos distribuidos de manera no secuencial, símbolos especiales compatibles con los sistemas institucionales, y combinaciones que no sigan patrones predecibles o fácilmente adivinables; y,

b) **Elementos Prohibidos.** Deben evitarse palabras de diccionario en cualquier idioma, información personal identificable como nombres, fechas de nacimiento o números de identificación, patrones secuenciales como "123456" o "abcdef", repeticiones de caracteres como "aaaaaa", combinaciones obvias como "password123", y cualquier información que pueda ser obtenida mediante ingeniería social o investigación en redes sociales.

IV. Buenas prácticas y controles adicionales

Una vez entregadas las contraseñas a cada usuario, cada uno se convierte en administrador de su cuenta, por lo cual una buena práctica es que cambien su contraseña por defecto a una que ellos seleccionen, y de preferencia esté en armonía con respecto con las políticas de contraseñas de la sección 3.

V. Responsabilidades

a) **Dirección de Servicios Tecnológicos y Plataforma Digital.** Tiene por responsabilidad mantener y actualizar el catálogo de gestores de contraseñas para uso institucional, asegurando que se cumplan con estándares de cifrado AES-256 o superiores. Establecer los lineamientos técnicos para la implementación de herramientas de gestión de credenciales. También ejecutar auditorías técnicas semestrales para evaluar el cumplimiento de los estándares establecidos y la efectividad de los controles implementados;

Además de estas, la Dirección de Servicios Tecnológicos también debe proporcionar asesoría continua al personal sobre configuración de autenticación multifactor, mejores prácticas para generación de contraseñas robustas y uso efectivo de gestores de contraseñas institucionales. Implementar y mantener herramientas automatizadas

para detectar contraseñas débiles, y reutilizar credenciales y patrones de autenticación inusuales. Coordinar los procedimientos de recuperación segura en casos de compromiso de credenciales; y,

b) **Usuarios en general.** Cada usuario es responsable de mantener la confidencialidad absoluta de sus credenciales, y cambiar las contraseñas por defecto al momento de recibir acceso. Deben utilizar exclusivamente los gestores de contraseñas aprobados institucionalmente y reportar inmediatamente cualquier sospecha de compromiso de sus credenciales. Están obligados a cumplir con los requisitos de longitud y complejidad establecidos según el tipo de cuenta asignada.

CAPÍTULO XVII
DE LA POLÍTICA PARA LA GESTIÓN DE CUENTAS INACTIVAS

CIS CONTROL #5: ADMINISTRACIÓN DE CUENTAS

I. Propósito y Objetivo

Establecer una política para la gestión proactiva y sistemática de cuentas de usuario y administrador que presenten períodos de inactividad prolongada. El objetivo de esta política es prevenir accesos no autorizados, reducir el área de ataque institucional, y mantener un entorno digital seguro y controlado mediante la identificación y trato apropiado de credenciales de acceso.

II. Alcances

Esta política se aplica a todas las cuentas de usuario y administrador dentro del ecosistema tecnológico de la SESEA, abarcando tanto los sistemas locales como las plataformas en la nube que forman parte de la infraestructura institucional. El alcance técnico incluye todos los servidores, estaciones de trabajo, aplicaciones, bases de datos, sistemas de correo electrónico y cualquier plataforma digital que requiera autenticación mediante credenciales institucionales.

El alcance se extiende a todos los tipos de cuentas existentes en la SESEA, desde cuentas de usuario general hasta cuentas administrativas con privilegios elevados.

III. Descripción de la política

Se considera cuenta inactiva aquella cuenta que no haya registrado actividad documentada de inicio de sesión, ejecución de comandos, acceso a archivos, o cualquier otra interacción con los sistemas institucionales durante un periodo de tiempo prolongado.

Este hecho puede ser respaldado a través del uso de logs de sistema en todas las plataformas y sistemas de la SESEA, relacionado con la cuenta en cuestión, sin tomar en consideración procesos automatizados o tareas programadas sin intervención humana directa.

En la administración de cuentas, se consideran dos criterios para deshabilitar cuentas de usuarios, estos dependen del tipo de cuentas y cantidad de días de inactividad.

a) **Cuenta General.** Aquellas cuentas de usuario estándar que no presenten actividad durante 60 días o más consecutivos, son clasificadas automáticamente como inactivas y sujetas a evaluación inmediata para determinación de acciones apropiadas.

   Las cuentas generales inactivas sin justificación operacional válida, deben ser deshabilitadas inmediatamente, preservando sus datos relacionados. Las cuentas generales de usuarios con desvinculación laboral no reportada proceden a eliminación permanente siguiendo protocolos de preservación de información crítica. Las cuentas generales con justificación temporal aprobada y que pasan la cantidad de días de inactividad, deben mantenerse en estado activo y con monitoreo con alertas automáticas para cualquier actividad; y,

b) **Cuenta Administrativa.** Las cuentas administrativas inactivas por más de 45 días son suspendidas automáticamente con notificación inmediata a la Secretaría Técnica. La reactivación requiere solicitud formal con justificación y aprobación por parte de la Secretaría Técnica y la Dirección de Servicios Tecnológicos y Plataforma Digital. Transcurridos 180 días sin justificación operacional, se va a proceder con la eliminación definitiva.

   Antes de la inhabilitación de una cuenta, se debe tratar de establecer contacto con el propietario de la cuenta a través del Departamento de Recursos Humanos, Financieros y Materiales esto con el fin de conocer su estatus laboral. Si la respuesta es afirmativa y se solicita más tiempo de inactividad, se puede extender el tiempo de espera, en caso contrato solo esperar a que termine el tiempo de inactividad.

   Posterior a la inhabilitación de una cuenta, es de suma importancia ejecutar un análisis de vulnerabilidad, donde se considere el nivel de privilegios de la cuenta inactiva, la accesibilidad a los diferentes sistemas, y el tiempo transcurrido desde la última actividad.

IV. **Responsabilidades**

Toda acción relacionada con gestión de cuentas inactivas debe documentarse en la bitácora correspondiente, la cual incluya identificación completa de la cuenta afectada, fecha del último acceso registrado en logs de auditoría, tipo de acción implementada (deshabilitación, eliminación, excepción), responsable técnico que ejecutó la acción, justificación específica cuando aplique, y referencias a documentación de soporte.

La Dirección de Servicios Tecnológicos y Plataforma Digital debe gestionar esta documentación, además de generar un reporte mensual de todas las acciones sobre cuentas inactivas se han detectado, e informar a la Secretaría Técnica, incluyendo métricas de cumplimiento, identificación de tendencias, y recomendaciones para mejoras en procesos.

CAPÍTULO XVIII

DE LA POLÍTICA PARA EL USO CORRECTO DE CUENTAS Y PRIVILEGIOS DE ACCESO, PRINCIPIO DE PRIVILEGIO MÍNIMO

CIS CONTROL #5: ADMINISTRACIÓN DE CUENTAS

I. **Propósito y Objetivo**

El propósito de esta política es establecer las directrices para el uso adecuado de cuentas de usuario general y usuaria administrativa en los sistemas de la SESEA, con el fin de fortalecer la seguridad informática, restringir permisos y evitar la utilización indebida de cuentas institucionales en sitios prohibidos.

II. **Alcance**

Esta política se aplica a todas las cuentas de usuario y administrador dentro del ecosistema tecnológico de la SESEA, abarcando tanto los sistemas locales como las plataformas en la nube que forman parte de la infraestructura institucional. El alcance técnico incluye todos los servidores, estaciones de trabajo, aplicaciones, bases de datos, sistemas de correo electrónico y cualquier plataforma digital que requiera autenticación mediante credenciales institucionales.

El alcance se extiende a todos los tipos de cuentas existentes en la SESEA, desde cuentas de usuario general hasta cuentas administrativas con privilegios elevados.

III. **Descripción de la política**

Las cuentas con privilegios administrativos con privilegios elevados, deberán mantenerse estrictamente separadas de las cuentas de usuario general. Cada administrador del sistema debe contar con dos cuentas distintas: una cuenta administrativa (por ejemplo, admin.nombre) con privilegios elevados, destinada exclusivamente para tareas de gestión del sistema, instalación de Software y mantenimiento de la red, y una cuenta de uso cotidiano (por ejemplo, nombre) sin privilegios, destinada al trabajo diario regular.

Las actividades comunes como navegación por Internet, envío y recepción de correo electrónico, edición de documentos y hojas de cálculo, participación en

reuniones virtuales y acceso a plataformas de colaboración como Zoom, Slack o Google Workspace, deben realizarse únicamente desde la cuenta de usuario general. Queda estrictamente prohibido utilizar la cuenta administrativa para estas actividades con el fin de reducir la exposición a riesgos de seguridad como malware, phishing y ataques dirigidos.

Por su parte, las cuentas de administrador tienen permisos para realizar tareas técnicas específicas en sistemas o equipos, por ende, solo deben ser utilizadas para:

a) Instalar o actualizar software autorizado;

b) Cambiar configuraciones del sistema operativo o red;

c) Administrar cuentas de otros usuarios (si el rol asignado lo permite); y,

d) Acceder a herramientas de administración del sistema o servidor.

Entre otras funciones, donde intervenga la gestión de usuarios o administración de sistemas informáticos.

Sin excepción, queda prohibido el uso de cuentas de general para este tipo de tareas de usuarios.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital, es la responsable de configurar y mantener la separación de cuentas, monitorear el uso adecuado de las mismas y realizar auditorías periódicas para asegurar el cumplimiento de esta política.

El personal que labora en la SESEA tiene la responsabilidad de no usar la cuenta asignada para usos no relacionados con sus actividades laborales, así como notificar a la Dirección de Servicios Tecnológicos cualquier incidente o acceso indebido.

CAPÍTULO XIX

DE LA POLÍTICA PARA LA GESTIÓN DE ACCESOS, PROCESO DE ALTAS, BAJAS Y CAMBIOS (PERMISOS)

CIS CONTROL #6: GESTIÓN DE CONTROL DE ACCESO

I. **Propósito y Objetivo**

En la presente política se establece el marco normativo y procedimental para la gestión de accesos, altas y bajas (permisos) de sistemas, plataformas o recursos de información de la SESEA. Con esta política se busca asegurar el principio de mínimos privilegios, garantizando así que cada usuario tenga únicamente los permisos necesarios para desempeñar sus funciones específicas, con el objeto de mantener un control de acceso adecuado y proporcional a las responsabilidades de cada puesto.

II. **Alcance**

Esta política aplica a todos los usuarios, que tengan acceso a los sistemas de información de la SESEA. El alcance incluye todas las cuentas institucionales, sistemas operativos, aplicaciones, plataformas web, servicios en la nube y dispositivos tecnológicos que requieran autenticación mediante credenciales de acceso.

La política abarca tanto cuentas de usuario estándar como cuentas administrativas y de alto privilegio, independientemente de si utilizan autenticación multifactor o no. Se incluyen también las cuentas de servicio, cuentas compartidas institucionales y cualquier sistema que maneje información sensible o crítica de la organización. Esta cobertura se extiende a todos los entornos tecnológicos, desde infraestructura local hasta servicios externos contratados que requieran credenciales institucionales.

III. **Descripción de la Política**

Durante el proceso de nueva contratación, cuando un colaborador se incorpora a la SESEA, necesita acceso inicial a los sistemas para desempeñar sus funciones. En casos de cambio de puesto o rol, sus responsabilidades se modifican y requieren ajustes en sus permisos de acceso. En este supuesto es donde entra en acción la

implementación de esta política. Para efectuar de manera correcta y coordinada la reasignación de permisos, se debe de tomar en consideración el procedimiento siguiente:

a) **Solicitud de acceso:** Para iniciar el jefe inmediato, responsable del área o el mismo colaborador según corresponda al caso específico, debe enviar una solicitud formal a la Dirección de Servicios Tecnológicos y Plataforma Digital. Esta solicitud debe incluir la justificación clara del acceso requerido y especificar el tipo de permisos necesarios. La solicitud puede realizarse a través de oficio formal, utilizando el formulario de solicitud de acceso establecido en el Anexo H, o mediante correo electrónico institucional dirigido a plataformadigital@seseamichoacan.mx, asegurando que toda la información requerida esté completa y sea precisa;

b) **Aprobación:** Toda solicitud debe seguir un proceso de aprobación que garantice la validación adecuada. La aprobación debe ser otorgada por la persona titular de la unidad administrativa del solicitante, quien conoce las necesidades específicas del puesto y puede validar la pertinencia del acceso solicitado. Adicionalmente, debe contar con la aprobación de la Secretaría Técnica. Finalmente, la Dirección de Servicios Tecnológicos y Plataforma Digital debe realizar la validación técnica y de seguridad correspondiente, asegurando que el acceso solicitado no comprometa la integridad del sistema ni exceda los niveles de privilegio apropiados;

c) **Otorgamiento de acceso:** Una vez aprobada la solicitud, la Dirección de Servicios Tecnológicos procede a crear las cuentas necesarias o modificar los permisos existentes según corresponda. Durante este proceso, se debe verificar meticulosamente que el acceso otorgado corresponda exactamente al rol real del usuario y a las funciones específicas que desempeña. Una vez habilitado el acceso, se notifica al usuario sobre los permisos concedidos, proporcionando información clara sobre sus responsabilidades en el uso de los recursos asignados y las políticas de seguridad que debe cumplir;

d) **Registro y documentación:** Toda concesión de acceso debe quedar debidamente registrada utilizando el formato establecido en el Anexo G. El registro debe incluir información completa y precisa como el nombre

completo del usuario, la fecha exacta de otorgamiento del acceso, el tipo específico de acceso concedido incluyendo sistema, nivel de privilegio y vigencia del mismo, así como la identificación de la persona o área que aprobó la solicitud. Estos registros deben ser mantenidos en resguardo por la Dirección de Servicios Tecnológicos por el periodo establecido por las políticas de retención institucionales: dos años para garantizar la trazabilidad y auditoría adecuada; y,

e) **Revisiones periódicas:** Se deben realizar revisiones periódicas con una frecuencia trimestral para mantener la integridad y actualización del sistema de accesos. Estas revisiones tienen como objetivo verificar que los accesos activos sigan siendo necesarios y apropiados para las funciones actuales de cada usuario. Durante este proceso se deben identificar y eliminar accesos obsoletos que puedan existir debido a cambios de rol, promociones, transferencias o salida de personal, asegurando que no persistan permisos innecesarios que puedan representar riesgos de seguridad.

IV. **Responsabilidades**

Los usuarios finales tienen la responsabilidad de solicitar el cambio de permisos, el cual debe estar justificado por sus funciones laborales, así como proteger adecuadamente sus credenciales y cumplir con las políticas de seguridad establecidas.

Las personas titulares de las unidades administrativas responsables deben aprobar los accesos, basándose estrictamente en las funciones del puesto, y la necesidad real del solicitante, ejerciendo un criterio responsable en la evaluación de cada solicitud.

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad integral de validar técnicamente las solicitudes, otorgar los accesos aprobados, mantener registros precisos y realizar las revisiones periódicas necesarias para asegurar el cumplimiento continuo de esta política.

V. **Normatividad de Referencia**

Esta política se fundamenta en los CIS Critical Security Controls v8, particularmente en el Control 6.1, que establece la necesidad de establecer y mantener un proceso formal para la asignación y gestión de accesos, con base en el principio de mínimos privilegios. Asimismo, se alinea con los estándares internacionales definidos por la norma ISO/IEC 27001, específicamente en los controles sobre seguridad lógica, y con la norma ISO/IEC 27002, en su Control 9.2: Gestión de acceso de usuarios, que establece directrices sobre la creación, modificación y revocación de derechos de acceso. Adicionalmente, se consideran las recomendaciones del NIST SP 800-53 Rev. 5, particularmente los controles AC-2 (Account Management) y AC-5 (Separation of Duties), que fortalecen la estructura organizativa del control de accesos.

CAPÍTULO XX
DE LA POLÍTICA PARA DESVINCULACIÓN O CAMBIO DE CUENTAS

CIS CONTROL #6: GESTIÓN DE CONTROL DE ACCESO

I. Propósito y Objetivo:

Establecer un proceso claro y eficiente para revocar de forma inmediata los accesos a sistemas, plataformas y recursos digitales cuando un colaborador deja la SESEA, cambia de función o pierde derechos de acceso por cualquier motivo. Este procedimiento garantiza la seguridad de la información institucional y el cumplimiento de las políticas de Ciberseguridad del presente Manual.

II. Alcance

Este procedimiento aplica de manera integral a todo el personal que mantenga credenciales o accesos a sistemas corporativos de la SESEA. Incluye empleados, personal contratado por honorarios, consultores externos, proveedores de servicios y cualquier tercero que tenga acceso autorizado a los recursos tecnológicos institucionales, independientemente de la modalidad contractual, el nivel jerárquico o el puesto que ostenten.

III. Descripción de la Política

La revocación de accesos procede en situaciones de baja de personal, incluyendo renuncia voluntaria, terminación de la relación laboral, despido justificado o injustificado, y finalización natural del período contractual. También aplica cuando ocurren cambios de puesto o función que impliquen modificación en los privilegios de acceso, ya sea por promoción, reubicación departamental o reestructuración organizacional. Asimismo, se ejecuta cuando existe revocación de derechos por decisión institucional, derivada de procesos disciplinarios, investigaciones internas, medidas precautorias, errores en la asignación inicial de permisos o cualquier circunstancia que comprometa la seguridad de la información.

IV. **Proceso de revocación**

a) **Notificación** a la Dirección de Servicios Tecnológicos. Toda solicitud relacionada con la revocación de accesos debe ser comunicada de manera inmediata y formal a la Dirección de Servicios Tecnológicos y Plataforma Digital. Esta notificación puede ser iniciada por el Departamento de Recursos Humanos, Financieros y Materiales en casos de movimientos de personal, o por el jefe directo del colaborador cuando se trate de situaciones específicas del área de trabajo. La comunicación debe realizarse a través de oficio institucional para casos formales, formulario de solicitud de acceso debidamente completado según el formato establecido en el Anexo H, o mediante correo electrónico institucional dirigido a plataformadigital@seseamichoacan.mx cuando la urgencia del caso así lo requiera;

b) **Tiempo de respuesta.** La Dirección de Servicios Tecnológicos tiene la responsabilidad de proceder con la revocación de accesos en un plazo máximo de cuatro horas laborales contadas a partir de la recepción formal de la notificación. Este tiempo permite ejecutar las acciones necesarias de manera ordenada y verificar que todos los accesos sean efectivamente revocados sin comprometer la operatividad de los sistemas institucionales; y,

c) **Acciones a realizar por la Dirección de Servicios Tecnológicos.** El personal técnico procederá a desactivar completamente las cuentas de red, incluyendo correo electrónico institucional, acceso al dominio institucional, conexiones VPN y cualquier otro servicio de conectividad. Simultáneamente, se revocará el acceso de todas las aplicaciones, plataformas y sistemas específicos que el colaborador tenía autorizados según su perfil de usuario, puesto o atribución. En los casos que corresponda, se coordinará la recuperación física de dispositivos móviles, equipos de cómputo o hardware especializado, o en su defecto, se procederá al bloqueo remoto de dichos equipos. Todas estas acciones quedarán debidamente documentadas en el registro de gestión de accesos establecido en el Anexo G.

V. **Validación.** Una vez completado el proceso de revocación, la Dirección de Servicios Tecnológicos debe confirmar formalmente la finalización exitosa de

todas las acciones realizadas. Esta confirmación se enviará al Departamento de Recursos Humanos, Financieros y Materiales, a la Delegación Administrativa y al jefe inmediato del colaborador, proporcionando la certeza de que los accesos han sido efectivamente revocados y que no existen vulnerabilidades residuales en el sistema.

VI. **Responsabilidades**

La Dirección de Servicios Tecnológicos es responsable de realizar las acciones correspondientes conforme al procedimiento descrito y dentro de los plazos establecidos. Corresponde al Departamento de Recursos Humanos, Financieros y Materiales notificar de manera formal y oportuna cualquier movimiento de personal que implique la revocación de credenciales, mientras que las áreas solicitantes, incluyendo jefes inmediatos y unidades administrativas, tienen la obligación de informar a la Dirección de Servicios Tecnológicos cuando ocurra cualquier modificación funcional que afecte los niveles de acceso. El cumplimiento efectivo de esta política depende de la coordinación entre todas las áreas involucradas y de la atención oportuna a las solicitudes de revocación.

VII. **Normatividad de Referencia**

Esta política se encuentra alineada con el Control 6.2 de los CIS Critical Security Controls v8, el cual establece la necesidad de revocar los accesos de usuarios cuando ya no se requieren, por razones de desvinculación, cambios de rol o modificación en privilegios. Asimismo, se vincula con los lineamientos de la norma ISO/IEC 27001:2022, específicamente con el control 5.18: Derechos de acceso y con el control 9.2.6 de la ISO/IEC 27002, relativo a la eliminación o desactivación de derechos de acceso en tiempo y forma. Complementariamente, se consideran las mejores prácticas establecidas en el NIST SP 800-53 Rev. 5, particularmente en el control AC-2, que recomienda la eliminación o desactivación inmediata de cuentas una vez terminada la necesidad operativa o contractual.

CAPÍTULO XXI
DE LA POLÍTICA DE USO DE AUTENTICACIÓN MULTIFACTOR (MFA)

CIS CONTROL #6: GESTIÓN DE CONTROL DE ACCESO

I. Propósito y Objetivo

Esta política establece la implementación obligatoria de autenticación multifactor (MFA) en todas las aplicaciones institucionales y de terceros que tengan exposición a Internet. El propósito fundamental es fortalecer la seguridad de los accesos digitales y añadir una capa de protección crítica para resguardar la información institucional. La autenticación multifactor reduce de forma significativa el riesgo de accesos no autorizados, incluso cuando las credenciales principales han sido comprometidas.

II. Alcance

Esta política aplica de forma universal a todos los sistemas y plataformas informáticas utilizadas por la SESEA, tanto aquellas desarrolladas internamente como las adquiridas a proveedores externos. Esto incluye aplicaciones accesibles desde redes públicas o remotas, tales como servicios de correo electrónico institucional, herramientas en la nube, plataformas colaborativas, portales con funciones de inicio de sesión y todos aquellos servicios que gestionen información sensible o confidencial. El alcance comprende también los accesos administrativos con privilegios elevados, así como las cuentas de usuario que interactúan con sistemas críticos o de alta disponibilidad operativa.

III. Descripción de la Política

La activación de mecanismos de autenticación multifactor se considera una medida de seguridad obligatoria y no sujeta a negociación, siempre que su implementación resulte viable técnicamente y operativamente. Esta obligatoriedad se fundamenta en la necesidad crítica de proteger los activos digitales institucionales contra amenazas cibernéticas cada vez más sofisticadas.

Su aplicación debe garantizarse como condición previa para la operación normal de sistemas, especialmente en entornos con acceso administrativo, aplicaciones expuestas a Internet, y servicios que almacenan, procesan o transmiten información clasificada como sensible. La autenticación multifactor no sustituye a otros controles de acceso, sino que los complementa, fortaleciendo la defensa contra intrusiones y accesos indebidos.

La autenticación multifactor deberá sustentarse en la combinación de al menos dos elementos distintos de verificación: algo que el usuario conoce, como una contraseña o PIN, y algo que el usuario posee, como una aplicación autenticadora instalada en su dispositivo móvil. En casos donde resulte técnica y operativamente viable, puede considerarse el uso de un tercer factor vinculado a características biométricas, como huella digital o reconocimiento facial, siempre y cuando el sistema lo permita de manera nativa y sin necesidad de adquisición de dispositivos externos.

Debido a las limitaciones del presupuesto institucional, no se contempla el uso de tokens físicos ni de dispositivos especializados de hardware como método de autenticación. En su lugar, se establece como opción preferente el uso de aplicaciones autenticadoras conocidas y gratuitas, tales como Microsoft Authenticator o Google Authenticator. Estas herramientas proporcionan un equilibrio adecuado entre facilidad de uso, seguridad y accesibilidad, y se consideran ampliamente efectivas para mitigar riesgos de acceso no autorizado. La autenticación mediante SMS solo deberá emplearse como último recurso y bajo criterios excepcionales, debido a su menor nivel de protección frente a ataques de suplantación o interceptación.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos es responsable de coordinar la implementación y supervisar el cumplimiento de los lineamientos aquí establecidos en materia de autenticación multifactor. Esta labor incluye asegurar que los sistemas institucionales contemplados en esta política adopten mecanismos efectivos de autenticación que respondan a las necesidades de seguridad de la organización, así como brindar el acompañamiento técnico necesario a las áreas involucradas para su correcta aplicación. Asimismo, corresponde a la Dirección de Servicios Tecnológicos monitorear el funcionamiento de las soluciones implementadas,

proponer mejoras continuas y atender, de manera oportuna, cualquier incidente o desviación que comprometa la integridad del modelo de autenticación multifactor.

En concordancia con esta política, los equipos de desarrollo de Software, ya sean internos o externos, deben incorporar la funcionalidad de autenticación multifactor desde la fase de diseño de cualquier sistema nuevo, asegurando que la arquitectura de las aplicaciones contemple esta medida como parte esencial de su modelo de seguridad. Para los sistemas existentes, deberán realizar un análisis técnico que determine la viabilidad de implementación, documentar cualquier limitación identificada y colaborar con la Dirección de Servicios Tecnológicos en la búsqueda de soluciones viables que mitiguen los riesgos asociados.

Los usuarios finales, independientemente de su nivel jerárquico o función dentro de la SESEA, están obligados a utilizar de forma adecuada y consistente el segundo factor de autenticación que les sea asignado. De igual manera, deberán notificar sin demora cualquier irregularidad, mal funcionamiento o situación sospechosa relacionada con los mecanismos de autenticación multifactor, con el fin de preservar la seguridad de los sistemas institucionales.

V. **Normativas de Referencia**

Esta política se basa en las mejores prácticas internacionales en materia de Ciberseguridad, específicamente en los CIS Controls v8, con énfasis en el Control 6.3, que establece la obligatoriedad de implementar autenticación multifactor para aplicaciones expuestas externamente. Asimismo, se alinea con los estándares definidos por la ISO/IEC 27001 y 27002, relativos a los controles de acceso y protección de activos de información.

Adicionalmente, sigue las recomendaciones técnicas del NIST SP 800-63B Digital Identity Guidelines, particularmente en lo que respecta a la implementación de múltiples factores de autenticación para accesos sensibles.

CAPÍTULO XXII

DE LA POLÍTICA DE SEGURIDAD PARA ACCESO REMOTO A LA RED CON AUTENTICACIÓN MULTIFACTOR (MFA)

CIS CONTROL #6: GESTIÓN DE CONTROL DE ACCESO

I. Propósito y Objetivo

Esta política establece los lineamientos técnicos y operativos para asegurar que todo acceso remoto a la red y a los sistemas institucionales de la SESEA se encuentre debidamente protegido mediante mecanismos de autenticación multifactor (MFA). Su objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de la información institucional frente a posibles accesos no autorizados derivados del robo de credenciales, ataques de fuerza bruta o cualquier otro tipo de amenaza cibernética. El uso de autenticación multifactor representa una medida crítica para reducir los riesgos asociados al acceso remoto, reforzando la postura de Ciberseguridad institucional mediante la implementación de un segundo factor de autenticación que complemente las credenciales principales del usuario.

II. Alcance

Esta política de seguridad aplica de manera integral a todo el personal que, en el ejercicio de sus funciones, requiera establecer conexiones remotas con los sistemas, redes, plataformas o servicios institucionales administrados por la Dirección de Servicios Tecnológicos, incluyendo empleados de base, personal eventual, prestadores de servicios, consultores y cualquier otro tercero autorizado.

Asimismo, la política abarca los entornos y herramientas tecnológicas que permitan la interacción con información institucional, así como aquellos sistemas desarrollados externamente que, al haber sido entregados a la Dirección de Servicios Tecnológicos para su gestión, mantenimiento y actualización, forman parte del ecosistema digital de la SESEA En todos estos casos, sin importar la ubicación del usuario o el tipo de dispositivo utilizado, el acceso remoto deberá contar obligatoriamente con mecanismos de autenticación multifactor conforme a los lineamientos establecidos en la presente política.

III. **Descripción de la Política**

La autenticación multifactor es obligatoria para todo acceso remoto a los sistemas, redes y servicios institucionales administrados por la Dirección de Servicios Tecnológicos. Su implementación es condición previa para cualquier conexión remota, sin distinción de jerarquía, perfil funcional o ubicación.

El segundo factor deberá basarse en mecanismos seguros, personales e intransferibles, como aplicaciones autenticadoras móviles (ej. Microsoft Authenticator o Google Authenticator) o notificaciones push en dispositivos previamente registrados. No se admitirán métodos inseguros u obsoletos, como tokens físicos o autenticación por SMS, salvo en situaciones excepcionales y debidamente justificadas.

Esta política aplica a cualquier tecnología de acceso remoto, incluyendo VPN (IPSec, SSL), servicios de escritorio remoto (RDP, VDI), portales web institucionales, servicios en la nube (SaaS, IaaS, PaaS), y herramientas de soporte remoto autorizadas como AnyDesk. En todos los casos, la activación de MFA será un requisito indispensable para garantizar la protección de la información y los activos digitales institucionales. La siguiente tabla resume los escenarios contemplados:

Tipo de acceso remoto	MFA requerido
VPN (IPSec, SSL, entre otros.)	Obligatorio
Escritorio remoto (RDP, VDI)	Obligatorio
Acceso remoto vía navegador	Obligatorio
Plataformas en la nube (SaaS, IaaS, PaaS.)	Obligatorio
Herramientas de soporte remoto (p. ej. AnyDesk)	Obligatorio

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos es responsable de configurar, implementar y mantener los mecanismos de autenticación multifactor en todos los sistemas y plataformas que permitan o requieran acceso remoto a la infraestructura digital de la SESEA. Esta responsabilidad comprende la selección de soluciones adecuadas, la aplicación de políticas técnicas, y la coordinación con las áreas usuarias y, en su caso, con proveedores externos, para asegurar su adopción efectiva.

Debido a las limitaciones presupuestales institucionales, no se contempla el uso de tokens físicos ni de dispositivos especializados de hardware como método de autenticación. En su lugar, se establece como opción preferida el uso de aplicaciones autenticadoras conocidas, gratuitas y ampliamente compatibles, tales como Microsoft Authenticator o Google Authenticator. Estas herramientas generan códigos de un solo uso que expiran al pasar cierto tiempo y se consideran efectivas, accesibles y suficientemente seguras para mitigar el riesgo de accesos indebidos.

En los casos en que el sistema lo permita de forma nativa, sin requerir dispositivos externos, podrá considerarse el uso de factores biométricos como huella digital o reconocimiento facial como segundo o tercer factor, siempre que su implementación no comprometa la operación o genere dependencias técnicas innecesarias.

El uso de mensajes SMS como segundo factor de autenticación no se recomienda, dada su vulnerabilidad frente a ataques de suplantación o interceptación. Sin embargo, en escenarios donde no existan alternativas viables o persistan las limitaciones técnicas, el uso de SMS podrá autorizarse de manera transitoria, bajo condiciones específicas y con base en un análisis de riesgos realizado por la Dirección de Servicios Tecnológicos.

V. **Normativas de Referencia**

Esta política se basa en las mejores prácticas internacionales en materia de Ciberseguridad, específicamente en los CIS Controls v8, con énfasis en el Control 6.4, que establece la obligatoriedad de exigir autenticación multifactor para accesos remotos a la red. Asimismo, se alinea con los estándares definidos por la ISO/IEC 27001 y 27002, particularmente en lo relativo al control de acceso, gestión de identidades y protección de activos de información.

Adicionalmente, considera las recomendaciones del NIST SP 800-63B Digital Identity Guidelines, con especial atención a las disposiciones técnicas aplicables a

la autenticación multifactor para usuarios que interactúan con sistemas institucionales de forma remota.

CAPÍTULO XXIII

DE LA POLÍTICA DE USO DE AUTENTICACIÓN MULTIFACTOR (MFA) EN CUENTAS ADMINISTRATIVAS

CIS CONTROL #6: GESTIÓN DE CONTROL DE ACCESO

I. Propósito y Objetivo

Esta política establece la obligación de implementar mecanismos de autenticación multifactor (MFA) para todas las cuentas administrativas dentro de la SESEA. Su objetivo es fortalecer la protección de accesos privilegiados a sistemas críticos mediante una capa adicional de seguridad, que complemente el uso de credenciales tradicionales y contribuya a reducir el riesgo de accesos no autorizados.

En un entorno donde las amenazas cibernéticas evolucionan de manera constante, la implementación de MFA representa una medida de seguridad esencial para proteger la integridad de los activos digitales institucionales, garantizar la trazabilidad de las acciones realizadas por personal autorizado y preservar la confidencialidad de la información sensible que resguarda la SESEA.

II. Alcance

Esta política aplica sin excepción a todas las cuentas que posean privilegios administrativos, sin importar el área responsable, la jerarquía de quien las utilice ni la ubicación desde donde se acceda. Incluye tanto a personal interno como a proveedores externos, contratistas y prestadores de servicios.

El alcance de esta política cubre servidores físicos y virtuales, equipos de cómputo con privilegios de administración, infraestructura de red (como routers, switches, firewalls y controladores inalámbricos), consolas de gestión en la nube (Google Cloud Platform), así como accesos de soporte técnico remoto brindados por terceros.

Es importante destacar que no se establece distinción alguna entre ambientes locales, servicios en la nube o esquemas híbridos: toda forma de acceso administrativo queda sujeta al cumplimiento obligatorio de los lineamientos aquí establecidos.

III. **Descripción de la Política**

Toda cuenta administrativa deberá utilizar autenticación multifactor como requisito indispensable para su operación. No se permitirá, bajo ninguna circunstancia, el acceso con privilegios administrativos empleando únicamente usuario y contraseña. Los mecanismos aprobados para cumplir con esta política serán las aplicaciones autenticadoras como Microsoft Authenticator y Google Authenticator, las cuales han sido adoptadas por la Dirección de Servicios Tecnológicos como soluciones oficiales, en virtud de su viabilidad técnica, disponibilidad, costo accesible y soporte institucional. El uso de tokens físicos ha sido descartado por limitaciones presupuestales.

Asimismo, las cuentas deberán ser de uso individual, estar debidamente identificadas y no podrán compartirse entre usuarios. Se promoverá el uso de mecanismos centralizados de autenticación que integren controles de acceso con autenticación multifactor, tales como directorios activos o soluciones institucionales de inicio de sesión único. En los casos en que un sistema no permita integrar este tipo de autenticación, se deberá documentar la situación, justificar técnicamente la excepción y presentar un plan de actualización progresiva con fechas definidas para su resolución.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos es responsable de definir, implementar y mantener los mecanismos de autenticación multifactor en todas las cuentas administrativas. Esta Dirección deberá asegurar que dichos mecanismos estén alineados con los estándares establecidos en el presente Manual, brindar soporte técnico a las áreas involucradas y supervisar su cumplimiento mediante procesos de monitoreo continuo.

Asimismo, la Dirección de Servicios Tecnológicos será responsable de mantener actualizados los registros de autenticación, vigilar el comportamiento de los accesos privilegiados y coordinar las acciones correctivas necesarias ante cualquier

incidente de seguridad o incumplimiento detectado. El personal con cuentas administrativas deberá observar en todo momento los lineamientos aquí establecidos, conservar la confidencialidad de sus credenciales, reportar anomalías y colaborar activamente en las revisiones técnicas o en la aplicación de mejoras.

Los proveedores externos que operen con acceso administrativo sobre los sistemas de la SESEA estarán obligados a cumplir con esta política como condición para la prestación de servicios. Su cumplimiento deberá establecerse contractualmente como un requisito explícito para conservar los privilegios de acceso.

V. **Normativas de Referencia**

Esta política se basa en las mejores prácticas internacionales en materia de Ciberseguridad, específicamente en los CIS Controls v8, con énfasis en el Control 6.5, que establece la obligatoriedad de implementar autenticación multifactor para cuentas con privilegios administrativos. Asimismo, se alinea con los estándares definidos por la ISO/IEC 27001 y 27002, relativos a los controles de acceso y protección de activos de información.

Adicionalmente, sigue las recomendaciones técnicas del NIST SP 800-63B Digital Identity Guidelines, particularmente en lo que respecta a la implementación de múltiples factores de autenticación para accesos sensibles.

CAPÍTULO XXIV
DE LA POLÍTICA PARA ESTABLECER UN PROGRAMA DE GESTIÓN DE VULNERABILIDADES

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. Propósito y Objetivo

Esta política tiene como propósito establecer un proceso eficiente para la gestión de vulnerabilidades en todos los sistemas, dispositivos y aplicaciones tecnológicas de la SESEA. A través de este marco de trabajo, se busca reducir significativamente el riesgo por parte de amenazas tanto internas como externas, para conservar la integridad, confidencialidad y disponibilidad de la información institucional.

II. Alcance

Esta política aplica de manera obligatoria a todos los activos tecnológicos que forman parte de la infraestructura de la SESEA. Esto incluye servidores físicos y virtuales, estaciones de trabajo de usuarios finales, dispositivos de red como routers y switches, todas las aplicaciones desarrolladas internamente o adquiridas de terceros, así como los sistemas alojados en servicios de nube pública o privada. También comprende cualquier dispositivo o sistema que maneje información sensible o que esté conectado directa o indirectamente a la red institucional.

III. Descripción de la política

Para la efectividad de esta política, se deben tener en cuenta los siguientes puntos para poder desarrollar un programa de gestión de vulnerabilidades adecuado.

a) **Identificación:** La identificación de vulnerabilidades se debe realizar de manera sistemática y planificada a través de escaneos automatizados. Estos escaneos deben ejecutarse periódicamente cada tres meses como parte del programa de mantenimiento preventivo. Adicionalmente, se debe realizar un escaneo inmediato después del despliegue de nuevos sistemas o cuando se implementen actualizaciones mayores que puedan introducir nuevas vulnerabilidades.

Para llevar a cabo estos escaneos, se deben utilizar herramientas especializadas como OpenVAS, Nessus, Qualys, o las herramientas propias proporcionadas por los proveedores de Software y hardware. La selección de la herramienta dependerá del tipo de activo a evaluar y la profundidad del análisis requerido;

b) **Análisis:** Una vez identificadas las vulnerabilidades, cada una debe ser analizada cuidadosamente considerando múltiples factores críticos. En primer lugar, se debe evaluar la gravedad utilizando el sistema CVSS (Common Vulnerability Scoring System) o los criterios establecidos por el proveedor del Software afectado. Posteriormente, se debe determinar el impacto potencial que la vulnerabilidad podría tener sobre las operaciones del negocio, considerando tanto la criticidad de los sistemas afectados como la sensibilidad de los datos que manejan.

   Es fundamental también evaluar el nivel de exposición del sistema vulnerable, determinando si se trata de un sistema con acceso local únicamente, si está expuesto a la red interna, o si tiene exposición directa a Internet. Finalmente, se debe verificar la existencia de ataques activos que estén aprovechando esta vulnerabilidad, utilizando fuentes de inteligencia de amenazas actualizadas;

c) **Priorización:** La priorización de vulnerabilidades es una escala de riesgo, donde se establecen tiempos máximos específicos para la mitigación. Las vulnerabilidades críticas requieren atención inmediata y deben ser corregidas dentro de las siguientes 48 horas. Las vulnerabilidades de nivel alto tienen un plazo de cinco días hábiles para su corrección, mientras que las de nivel medio deben ser atendidas dentro de 15 días hábiles. Las vulnerabilidades de nivel bajo pueden ser programadas para corrección dentro de 30 días hábiles o durante la próxima ventana de mantenimiento programado.

   Es importante destacar que estos tiempos pueden ajustarse según las circunstancias específicas, especialmente cuando las vulnerabilidades afectan sistemas críticos para la operación de la SESEA. En tales casos, la prioridad se incrementa automáticamente independientemente de la clasificación inicial de la vulnerabilidad;

d) **Corrección:** La corrección de vulnerabilidades se debe abordar mediante diferentes estrategias según la naturaleza del problema identificado. La primera opción es usar parches oficiales o actualizaciones proporcionadas por los fabricantes del Software. Cuando esto no sea posible, se pueden implementar cambios de configuración que mitiguen el riesgo asociado con la vulnerabilidad;

En casos donde los sistemas sean obsoletos y no tengan soporte del fabricante, se debe evaluar la sustitución del sistema por una versión más reciente o, como medida temporal, implementar el aislamiento del sistema vulnerable. Cuando ninguna de las opciones anteriores sea viable inmediatamente, se deben implementar controles compensatorios que reduzcan el riesgo mientras se trabaja en una solución definitiva; y,

e) **Validación:** Después de implementar cualquier corrección, es esencial validar que la vulnerabilidad haya sido efectivamente eliminada. Esto se logra realizando un nuevo escaneo automatizado o una prueba manual específica del sistema corregido. Una vez confirmado que la vulnerabilidad ya no está presente, se debe documentar detalladamente la acción correctiva realizada en el registro oficial de vulnerabilidades, incluyendo evidencia de la corrección exitosa.

Todas las vulnerabilidades identificadas deben ser registradas meticulosamente en una bitácora centralizada o sistema de gestión especializado. Este registro puede implementarse utilizando herramientas como Excel, sistemas de tickets como Jira, o integrarse con herramientas SIEM (Security Information and Event Management) para un enfoque más automatizado.

Cada registro debe contener información completa que incluya la fecha exacta de detección de la vulnerabilidad, el responsable asignado para su corrección, las fechas de corrección y validación, y toda la evidencia pertinente como logs del sistema, capturas de pantalla y reportes detallados del proceso de corrección.

IV. Responsabilidades

La Dirección de Servicios Tecnológicos tiene la responsabilidad principal de coordinar los escaneos periódicos, realizar el análisis técnico de las vulnerabilidades identificadas, y mantener el seguimiento continuo del proceso de gestión.

CAPÍTULO XXV

DE LA POLÍTICA PARA GENERAR ACTA DE REVISIÓN DEL PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. **Propósito y Objetivo**

Esta política tiene como propósito documentar formalmente el procedimiento de gestión de vulnerabilidades de algún activo tecnológico. Esta comprobación de vulnerabilidades se debe realizar de manera periódica o cuando las circunstancias organizacionales y tecnológicas lo requieran, asegurando así que el procedimiento permanezca vigente, efectivo y alineado con las mejores prácticas de Ciberseguridad.

II. **Alcance**

Este procedimiento aplica a todos los componentes del sistema de gestión de vulnerabilidades de la SESEA, abarcando tanto los aspectos técnicos como los procesos administrativos relacionados. El alcance incluye la evaluación de herramientas de detección y análisis de vulnerabilidades, los procedimientos de clasificación y priorización de riesgos, así como los protocolos de respuesta y remediación. También contempla las responsabilidades del personal involucrado, la efectividad de los canales de comunicación establecidos y la adecuación de los tiempos de respuesta definidos. Este alcance se extiende a todas las áreas de la organización que manejan activos de información críticos y abarca tanto la infraestructura física como los entornos virtuales y de nube que forman parte del ecosistema tecnológico institucional.

III. **Detalles de la política**

La política de gestión de vulnerabilidades se fundamenta en un sistema de revisión documental donde se captura la información importante para asegurar la efectividad y vigencia del procedimiento. Esta revisión trasciende el ámbito administrativo, y se constituye en una evaluación de la efectividad de los controles de seguridad implementados. El proceso de revisión permite identificar brechas en la protección,

evaluar la eficiencia de las herramientas utilizadas y determinar la necesidad de ajustes estratégicos en el enfoque de gestión de vulnerabilidades.

El motivo de la revisión puede surgir de diversas circunstancias; estas pueden ser revisiones anuales, mensuales, o bien por algún periodo definido, o bien, pueden surgir por la incorporación de nuevas tecnologías. Este hecho representa uno de los catalizadores más frecuentes para la actualización de los procedimientos, ya que demanda la integración de herramientas de detección más avanzadas, la implementación de metodologías de análisis innovadoras y la adaptación de los criterios de evaluación a las nuevas superficies de ataque.

En cualquier circunstancia que sea, se debe documentar todo el proceso, con respecto de los cambios realizados durante cada revisión. Esta documentación abarca desde la fecha de revisión, la cual representa el momento específico en que se realiza una evaluación integral del procedimiento, tanto los componentes técnicos como los aspectos operativos que requieren actualización o mejora continua, las actualizaciones de herramientas especializadas hasta la instalación de nuevos controladores de seguridad, modificaciones en los procedimientos de respuesta a incidentes y ajustes en los criterios de clasificación y priorización de vulnerabilidades. Toda esta información debe ser escrita en un tabla similar a la que se muestra a continuación:

Campo	Información
Fecha de revisión	[Ej. 18 de mayo de 2025]
Motivo de la revisión	☐ Revisión anual ☐ Cambio organizacional ☐ Nueva tecnología ☐ Otro: _____
Cambios realizados	[- Se actualizó herramienta de …. se instalaron nuevos controladores …]
Responsable de la revisión	[Nombre – Cargo]
Aprobado por	[Nombre – Responsable de Seguridad]

Próxima revisión prevista	[Fecha estimada]

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de dar seguimiento a las revisiones de procedimientos, así como su administración y gestión documental.

CAPÍTULO XXVI

DE LA POLÍTICA PARA REALIZAR ESCANEOS DE VULNERABILIDADES Y PRIORIZAR ESTRATEGIAS DE REMEDIACIÓN

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. Propósito y Objetivo

Esta política tiene como finalidad establecer una estrategia integral para la identificación, priorización y atención de vulnerabilidades que se pueden encontrar en la infraestructura tecnológica de la SESEA. El objetivo de esta política es garantizar que dichas vulnerabilidades sean remediadas de manera eficaz, oportuna y que estén completamente documentadas.

Con la implementación de esta política se busca lograr un ambiente tecnológico resiliente, así como reducir las áreas vulnerables de ataque y fortalecer la seguridad de las instalaciones tecnológicas.

II. Alcance

Esta política aplica a todos los activos tecnológicos de la SESEA, incluyendo servidores físicos y virtuales, estaciones de trabajo, equipos de red, aplicaciones web y móviles, sistemas en la nube y plataformas utilizadas por la SESEA.

III. Descripción de la política

La gestión de vulnerabilidades se fundamenta en la urgencia de atención o priorización basada en el riesgo que conlleva cada vulnerabilidad, esto para asignar recursos computacionales de manera eficiente, y con esto garantizar que las amenazas más significativas sean atendidas con la mayor urgencia.

Los factores considerados para la priorización de las vulnerabilidades deben incluir la puntuación CVSS (Common Vulnerability Scoring System), la cual proporciona una medida estandarizada de la gravedad técnica de la vulnerabilidad, a partir de este valor se puede evaluar el impacto potencial sobre los procesos. A través de

esta medida estandarizada se puede detectar el nivel de atención que requiere dicha vulnerabilidad. Estos niveles corresponden a la valoración siguiente:

a) **Nivel Crítico.** Las vulnerabilidades clasificadas como críticas son aquellas con puntuación CVSS igual o superior a 9.0, especialmente cuando afectan sistemas expuestos públicamente y existe evidencia de ataques en curso. Estas vulnerabilidades representan un riesgo muy alto que debe ser atendido de manera inmediata, dentro de un plazo máximo de 48 horas desde su detección;

b) **Nivel Alto.** Las vulnerabilidades de nivel alto comprenden aquellas con puntuación CVSS entre 7.0 y 8.9, estas vulnerabilidades representan un riesgo significativo para la seguridad de la información o la continuidad operativa, pero no requieren atención inmediata como las críticas, su remediación debe completarse dentro de cinco días hábiles para prevenir su escalamiento o explotación;

c) **Nivel Medio.** Este nivel de vulnerabilidades oscila entre 4.0 y 6.9 CVSS, generalmente estas vulnerabilidades no afectan sistemas o tienen un impacto limitado en las operaciones. Su remediación debe completarse dentro de 15 días hábiles, permitiendo una planificación adecuada de los recursos necesarios; y,

d) **Nivel Bajo.** Las vulnerabilidades de nivel bajo son aquellas con puntuación CVSS inferior a 4.0, estas vulnerabilidades presentan un impacto mínimo y generalmente no tienen exposición externa. Su corrección puede realizarse dentro de 30 días hábiles o durante la próxima ventana de mantenimiento programado.

En el supuesto de detectar alguna vulnerabilidad o tener indicios de alguna de ellas, se deben seguir los siguientes pasos para poder corregirla lo antes posible.

a) **Detección.** La detección constituye la fase inicial del ciclo de gestión de vulnerabilidades y tiene como propósito identificar de manera oportuna cualquier debilidad o fallo de seguridad presente en los activos tecnológicos. Esta identificación temprana es fundamental para prevenir la explotación de vulnerabilidades por parte de actores maliciosos.

La detección a seguir se basa en dos tipos complementarios de escaneos. Los escaneos periódicos completos que se deben realizar cada tres meses como parte del programa de mantenimiento preventivo, abarcando todos los activos tecnológicos, incluyendo servidores, dispositivos de red, aplicaciones web y estaciones de trabajo. Este tipo de escaneo permite establecer una línea base del estado de seguridad y detectar vulnerabilidades que puedan haber surgido durante el período transcurrido.

El segundo tipo de escaneo se conoce como escaneo ad-hoc, este escaneo se ejecuta de forma inmediata en respuesta a eventos como la implementación de nuevos sistemas o aplicaciones, la realización de actualizaciones o parches importantes, cambios en la configuración de red, apertura de nuevos puertos, exposición de servicios a Internet, o ante incidentes de seguridad y alertas de amenazas detectadas. El objetivo de este escaneo es identificar vulnerabilidades que puedan haber sido introducidas por cambios recientes en la infraestructura.

Para la detección se pueden utilizar herramientas como OpenVAS (Greenbone Vulnerability Management), Nessus de Tenable, Threat Intelligence y Qualys Vulnerability;

b) **Análisis de Criticidad.** Una vez detectadas las vulnerabilidades, se procede a analizarlas para determinar su impacto potencial y el nivel de riesgo que representan para la SESEA. En esta evaluación se deben considerar múltiples factores técnicos para determinar adecuadamente el impacto de cada vulnerabilidad, y se debe utilizar la puntuación CVSS (Common Vulnerability Scoring System) para clasificar la gravedad en una escala de 0.0 a 10.0,

El resultado de esta fase es una valoración técnica de cada vulnerabilidad, incluyendo una clasificación preliminar del riesgo como crítica, alta, media o baja, junto con la justificación de la clasificación considerando los criterios mencionados y observaciones específicas cuando sea el caso;

c) **Priorización.** Con base en el análisis de criticidad, se procede a la clasificación de vulnerabilidades según los niveles de riesgo establecidos

y la asignación de tiempos de respuesta máximos correspondientes. Durante esta fase se debe otorgar consideración especial a los mayores riesgos, excepto, si el daño se percibe en activos informáticos que podrían causar más problema a largo plazo, a pesar de tener una baja puntuación;

d) **Asignación a Responsables.** Cada vulnerabilidad priorizada se debe registrar en la bitácora o sistema de gestión correspondiente, incluyendo toda la información relevante para su seguimiento. Y se debe notificar a la Secretaría Técnica, proporcionando todos los detalles necesarios para proceder con la remediación, incluyendo recomendaciones específicas y recursos adicionales que puedan ser útiles;

e) **Remediación.** En la remediación se incluye la aplicación de parches de seguridad, cambios en configuraciones, aislamiento de sistemas afectados, o cualquier otra medida correctiva apropiada para eliminar o mitigar la vulnerabilidad. En casos donde la remediación inmediata no sea posible debido a restricciones operativas o técnicas, se deben implementar controles compensatorios temporales para reducir el riesgo mientras se planifica la corrección definitiva;

f) **Verificación.** Una vez completada la remediación, se procede a re-escanear o verificar manualmente la eliminación o mitigación completa de la vulnerabilidad. En esta verificación se debe confirmar que la corrección fue efectiva, y que no se introdujeron nuevas vulnerabilidades o problemas en el proceso. La información que se obtenga se debe adjuntar como evidencia documental.

En caso de obtener nuevas verificaciones se debe volver a iniciar el ciclo, comenzando por realizar un nuevo escaneo a los activos informáticos; y,

g) **Registro de Actividades.** Cada vulnerabilidad debe documentarse comprehensivamente, incluyendo la fecha de detección, nivel de criticidad asignado, responsable asignado para la remediación, fecha de remediación completada, fecha de validación de la corrección y evidencia adjunta que respalde la resolución exitosa.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de coordinar los escaneos de vulnerabilidades, realiza el análisis de criticidad y supervisa el proceso de validación de las correcciones implementadas. También tiene por responsabilidad ejecutar las actualizaciones de sistemas y aplicaciones, autorizar las modificaciones en entornos críticos, siempre y cuando las correcciones no afecten negativamente las operaciones bajo su responsabilidad.

CAPÍTULO XXVII
DE LA POLÍTICA PARA REALIZAR LA ACTUALIZACIÓN DE SISTEMAS OPERATIVOS

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. Propósito y objetivo

Establecer un procedimiento eficiente para la aplicación oportuna de parches de seguridad y actualizaciones de los sistemas operativos de los equipos tecnológicos, de la SESEA. Con este procedimiento se busca reducir significativamente la exposición a vulnerabilidades, para garantizar que todos los sistemas operativos mantengan niveles óptimos en protección contra amenazas cibernéticas emergentes y vulnerabilidades previamente identificadas.

II. Alcance

Este procedimiento aplica de manera integral a todos los sistemas operativos instalados en el ecosistema tecnológico de la SESEA. La cobertura incluye servidores físicos y virtuales, estaciones de trabajo institucionales utilizadas por el personal, equipos de red con sistemas operativos integrados como firewalls, routers y switches que forman parte de la infraestructura de conectividad, así como equipos móviles institucionales cuando corresponda. La aplicación de este procedimiento asegura que ningún componente tecnológico quede desprotegido ante vulnerabilidades conocidas.

III. Descripción de la política

La gestión de las actualizaciones se debe ejecutar bajo dos modalidades de frecuencia; Mensualmente, para recibir actualizaciones al menos una vez al mes durante las ventanas de mantenimiento programadas, y urgente, que se activa cuando se detectan vulnerabilidades, o cuando se identifican amenazas activas que requieren respuesta inmediata. En estos casos, los parches se aplican de forma inmediata sin esperar el ciclo mensual regular.

La obtención de actualizaciones se debe realizar exclusivamente a través de fuentes oficiales y verificadas. Para sistemas Windows se utiliza el Microsoft Update,

mientras que para sistemas Linux se recurre a los repositorios oficiales según la distribución correspondiente, incluyendo Ubuntu, RHEL y Debian. Los fabricantes de hardware y software como HP, Dell, Cisco y Fortinet proporcionan actualizaciones específicas para sus equipos, complementando las fuentes del sistema operativo. Adicionalmente, se deben consultar boletines de seguridad como CVE, NVD y CERT para mantenerse informado sobre vulnerabilidades emergentes y sus respectivas correcciones.

Para instalar actualizaciones a los Sistemas Operativos de los equipos tecnológicos de la SESEA, se deben considerar al menos los puntos siguientes:

a) **Identificación de parches disponibles.** La identificación de parches disponibles se debe realizar mediante revisiones semanales de todas las fuentes oficiales y boletines de seguridad relevantes. Durante este proceso se valida cuidadosamente la aplicabilidad de cada parche a los sistemas específicos en uso dentro de la organización, considerando versiones, configuraciones y dependencias particulares de cada activo tecnológico;

b) **Evaluación del impacto.** Se debe realizar una evaluación de impacto, donde se analicen detalladamente las implicaciones de la actualización, considerando el nivel de riesgo que representa la vulnerabilidad que corrige. Se debe validar exhaustivamente la compatibilidad de los sistemas actuales para evitar conflictos o interrupciones no planificadas, y se debe determinar si la instalación requiere reinicio del sistema, porque esta acción puede afectar la disponibilidad de la operación institucional;

c) **Programación de la instalación:** Se debe programar la instalación de las actualizaciones a modo que dicha actividad tenga el menor impacto operativo. En casos donde se requiera atención urgente debido a vulnerabilidades críticas, las instalaciones se deben programar fuera del horario laboral regular;

d) **Aplicación de la actualización:** La actualización se debe ejecutar utilizando herramientas automatizadas como WSUS, SCCM, scripts personalizados o Ansible cuando sea posible, o mediante procesos manuales cuando las herramientas automatizadas no sean aplicables; y,

e) **Pruebas post-parcheo:** Se deben realizar pruebas posteriores a la instalación para garantizar que los sistemas continúen funcionando correctamente, así como realizan verificaciones funcionales de los servicios y, ejecutar escaneos de verificación para confirmar que la vulnerabilidad ha sido efectivamente mitigada y no persisten riesgos residuales.

La ejecución de cada una de estas actividades debe quedar meticulosamente registrada en una bitácora institucional, donde se preserve la trazabilidad completa del proceso. El registro incluye la fecha exacta de instalación, identificación del activo actualizado, clasificación del tipo de actualización aplicada ya sea de seguridad, funcionalidad o emergencia, identificación del responsable que ejecutó la acción, y evidencia documental como reportes de herramientas, logs de sistema, capturas de pantalla o informes de revisión que respalden la correcta ejecución del proceso.

Cuando una actualización no pueda aplicarse debido a razones técnicas válidas o incompatibilidades del sistema, se debe documentar exhaustivamente la justificación técnica que impide la instalación. En estos casos se deben implementar controles compensatorios alternativos como aislamiento de red, configuración de firewall específica, segmentación de sistemas o monitoreo intensivo para mitigar los riesgos asociados a la vulnerabilidad no corregida. Paralelamente, se debe programar la corrección definitiva del problema o la sustitución del sistema afectado en el menor tiempo posible.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de coordinar el proceso de actualización de sistemas operativos, realizar el análisis de riesgo, y realizar validaciones post-parcheo para garantizar la correcta funcionalidad de los sistemas. Adicionalmente, debe ejecutar la instalación física de parches en los activos tecnológicos siguiendo los procedimientos establecidos y manteniendo la documentación requerida.

Las personas servidoras públicas que laboran en la SESEA tienen la responsabilidad de validar el funcionamiento correcto de los sistemas posteriores a las actualizaciones, reportando cualquier anomalía detectada, y proporcionan autorización para la aplicación de parches en sistemas críticos bajo su

responsabilidad, considerando el impacto operativo y los tiempos de implementación más apropiados.

CAPÍTULO XXVIII
DE LA POLÍTICA DEL PROCESO DE ACTUALIZACIONES AUTOMÁTICAS

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. Propósito y Objetivo

Establecer un procedimiento para garantizar que todas las aplicaciones instaladas en los activos tecnológicos de la SESEA se mantengan actualizadas de manera regular.

II. Alcance

Este procedimiento es aplicable a la totalidad de las aplicaciones instaladas en el ecosistema tecnológico de la SESEA. Se incluyen las estaciones de trabajo donde operan herramientas cotidianas como navegador web, clientes de correo electrónico, y plataformas de videoconferencia. También abarca los servidores que alojan componentes como motores de bases de datos, y aplicaciones desarrolladas internamente. Asimismo, contempla las herramientas administrativas que incluyen sistemas de respaldo, monitoreo de red y acceso remoto, entre otras aplicaciones que soporten las operaciones diarias de la organización.

III. Descripción de la política

La gestión de actualizaciones se debe ejecutar bajo dos modalidades:

a) Modalidad mensual, la cual debe contar con una revisión programada y sistemática para validar la disponibilidad de nuevas versiones y proceder con la aplicación de actualizaciones correspondientes; y

b) Modalidad ad-hoc la cual se activa cuando son liberados parches correctivos al software.

Para gestionar correctamente las actualizaciones automáticas, se debe cumplir con los pasos siguientes:

a) **Identificación de actualizaciones disponibles:** El primer paso es identificar las actualizaciones disponibles a través de canales seguros. Para ello se debe realizar una comprobación constante en los portales oficiales de los proveedores de software para detectar nuevas versiones y parches de seguridad. Complementariamente a esto, se pueden emplear herramientas automatizadas como PDQ Deploy, Chocolatey, scripts personalizados o Windows Server Update Services (WSUS). Esta etapa se puede mejorar si se reciben suscripciones, boletines de seguridad directamente por fabricantes reconocidos;

b) **Evaluación de riesgo:** Una vez identificadas las actualizaciones disponibles, se procede con un análisis del impacto potencial que cada parche o actualización podría generar en la funcionalidad operativa de los sistemas, a partir de este análisis se procede con la calendarización para instalar dichas actualizaciones;

c) **Planeación y pruebas:** La fase de planeación establece que todas las actualizaciones deben someterse a pruebas exhaustivas en entornos controlados antes de proceder con el despliegue masivo en el ambiente productivo. Este proceso de validación previa es fundamental para identificar posibles conflictos o incompatibilidades que puedan afectar la operación normal de los sistemas;

d) **Aplicación:** La implementación de las actualizaciones se debe ejecutar mediante herramientas dedicadas cuando sea técnicamente factible o a través de instalación manual en casos que requieran intervención especializada; y,

e) **Verificación:** La fase de verificación confirma si la actualización se ha implementado correctamente, en caso de ser afirmativo, se ejecutan pruebas de funcionalidad post-actualización, para asegurar que las aplicaciones operan según los parámetros esperados. En casos donde la actualización respondía a una vulnerabilidad específica, se verifica que la mitigación haya sido efectiva y que el riesgo de seguridad haya sido adecuadamente controlado.

Cada intervención realizada en el marco de este procedimiento debe quedar documentada de manera exhaustiva para garantizar la trazabilidad y control de las

modificaciones aplicadas. El registro incluye la fecha exacta de la actualización, el nombre completo y versión de la aplicación intervenida, la identificación específica de los equipos donde se aplicó la actualización, el responsable técnico que ejecutó la acción y la evidencia correspondiente que puede incluir capturas de pantalla, archivos de log del sistema o reportes generados por las herramientas utilizadas. Esta documentación sirve como base para auditorías internas y facilita la resolución de incidencias que puedan surgir posteriormente.

En el supuesto de que existan herramientas de software que no se deban actualizar debido a incompatibilidades en las librerías. Estas herramientas deben contar con la aprobación de la Dirección de Servicios Tecnológicos antes de proceder con cualquier modificación y se debe documentar el análisis detallado de incompatibilidad, en el cual se evalúe el impacto de la actualización propuesta, garantizando así que no se comprometa la estabilidad operativa de los procesos por dicha herramienta.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital asume la coordinación del proceso de detección de nuevas versiones disponibles, realiza la evaluación de riesgo y aprueba la implementación de actualizaciones que requieren aplicación inmediata. Esta misma dirección ejecuta la instalación de dichas actualizaciones, documenta todas las acciones realizadas y lleva a cabo las pruebas post-actualización necesarias para verificar la correcta implementación.

Por su parte, el personal de la SESEA tiene la responsabilidad de validar la compatibilidad funcional de las aplicaciones y proporcionar la retroalimentación necesaria para garantizar que las actualizaciones no comprometan la operatividad de sus procesos de trabajo.

CAPÍTULO XXIX

DE LA POLÍTICA DE CONSERVACIÓN Y RETENCIÓN DE REGISTROS DE SEGURIDAD

CIS CONTROL #7: GESTIÓN CONTINUA DE VULNERABILIDADES.

I. Propósito y Objetivo

Establecer y mantener un proceso enfocado a la gestión de registros que surjan en los activos tecnológicos de la SESEA. Este proceso tiene como finalidad asegurar la trazabilidad completa de las acciones realizadas en los sistemas, facilitar la detección oportuna de incidentes de seguridad, garantizar el cumplimiento de los requisitos legales aplicables y mantener la integridad de los sistemas de información institucionales.

II. Alcance

Esta política se aplica a todos los sistemas, aplicaciones, dispositivos de red, plataformas en la nube y servicios que forman parte de la infraestructura tecnológica de la SESEA. El alcance incluye tanto sistemas críticos como de soporte, abarcando plataformas de almacenamiento, comunicaciones y cualquier activo tecnológico que procese, almacene o transmita información institucional.

III. Descripción de la política

Para que sea efectiva la gestión de registros, se debe implementar un sistema de registro robusto que capture eventos en todos los activos tecnológicos, esto para permitir la recolección de datos valiosos, tal y como se solicitan en el Anexo I. Estos datos se obtienen de diferentes eventos, como lo son:

a) Eventos Mínimos a Registrar

1. **Autenticación de usuarios:** Se registrarán todos los eventos relacionados con el acceso al sistema, incluyendo inicios y cierres de sesión exitosos, intentos fallidos de acceso que puedan indicar actividad maliciosa, y bloqueos automáticos de cuentas por políticas de seguridad;

2. **Cambios en configuraciones:** Se documentarán todas las modificaciones realizadas a elementos sensibles del sistema, como cambios en reglas de firewall, actualizaciones de políticas de contraseñas, modificaciones en privilegios de usuario y ajustes en configuraciones de seguridad;

3. **Accesos a información sensible o confidencial:** Será monitoreado el acceso a bases de datos que contengan información ciudadana, documentos de investigación, archivos confidenciales y cualquier información clasificada según los niveles de sensibilidad institucionales;

4. **Ejecución de comandos administrativos:** Se registrará el uso de privilegios elevados, incluyendo comandos ejecutados con permisos de sudo/root en sistemas Linux o acciones realizadas con privilegios de administrador en sistemas Windows;

5. **Errores del sistema y fallos de aplicaciones:** Se documentarán las caídas del sistema, y excepciones que afecten la operación, reinicios inesperados y cualquier anomalía que comprometa la disponibilidad de los servicios; y,

6. **Acciones de mantenimiento:** Se registrarán las actividades de mantenimiento programado, incluyendo la aplicación de parches de seguridad, actualizaciones de Software y cambios de versión que puedan afectar la configuración del sistema.

b) Recolección de Registros

- **Fuentes de Registro:** Los sistemas operativos proporcionarán registros a través de herramientas como Windows Event Viewer y journald en sistemas Linux;

- **Los dispositivos de red**, incluyendo firewalls y routers, proporcionarán eventos relacionados con el tráfico de red e intentos de acceso no autorizado. Las plataformas en la nube generarán logs de Identity and Access Management (IAM), registro de

funciones ejecutadas y objetos accedidos. Los sistemas de respaldo mantendrán bitácoras detalladas de las tareas ejecutadas y los resultados de verificación de integridad; y,

- **Herramientas y Formatos:** La recolección se realizará de manera automática mediante agentes especializados, utilizando protocolos estándar como Syslog, sistemas SIEM (Security Information and Event Management) y herramientas como Wazuh para la gestión centralizada. Los registros se almacenarán en formatos estándar como JSON, CSV o archivos planos debidamente protegidos para garantizar su integridad y facilitar su análisis posterior. Cuando sea aplicable, se utilizarán consolas o repositorios centralizados para consolidar la información de múltiples fuentes.

Para mantener un orden, se deben realizar revisiones de registros frecuentemente. Estas revisiones se deben de implementar de acuerdo con la tabla siguiente:

Tipo de Evento	Frecuencia mínima de revisión
Accesos y autenticaciones	Diaria, mediante alertas automáticas.
Cambios críticos y errores del sistema	Semanal, análisis por personal técnico.
Reportes consolidados	Mensual, análisis de tendencias y anomalías.

En la siguiente tabla se muestran los periodos de conservación de registros.

Tipo de Registro	Tiempo de Conservación	Observaciones
Registros de seguridad (logs de eventos del sistema)	2 años	Recomendación ISO 27001 y alineado a auditorías anuales o bianuales.
Accesos a información sensible (datos personales/confidenciales)	2 años	Por requerimientos de trazabilidad y responsabilidad administrativa.

Errores de sistema y fallos críticos	1 año mínimo	Puede ampliarse si hubo incidentes.
Cambios en configuración o administración	2 años	Incluye modificaciones a permisos, roles, políticas, reglas de firewall, entre otros.
Registros de respaldo (logs de respaldo/restore)	1 año	Para análisis de disponibilidad y cumplimiento de políticas de backup.

Una vez que los registros excedan su tiempo de vida, se deben eliminar. A excepción de que estén relacionados con incidentes o investigaciones activas, en ese supuesto deben conservarse hasta la conclusión del caso. De otro modo, se deben eliminar conforme al "Procedimiento para la Eliminación Segura de Datos según su Nivel de Sensibilidad". Con este proceso se garantiza que la información no pueda ser recuperada mediante técnicas de borrado seguro, sobrescritura múltiple o destrucción criptográfica. La eliminación debe quedar documentada con fecha, tipo de registro y responsable según el formato establecido en el Anexo D.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos tiene la responsabilidad principal de definir las políticas de registro, monitorear los eventos de seguridad y gestionar tanto la revisión como la conservación de los registros. Adicionalmente, debe configurar, habilitar y proteger los registros en cada sistema bajo su administración. Así como validar los registros generados por sus aplicaciones y alertar sobre cualquier anomalía que pueda comprometer la seguridad o funcionamiento del sistema. La Dirección de Servicios Tecnológicos debe analizar los errores de funcionamiento y accesos indebidos para determinar las acciones correctivas necesarias. Las auditorías internas o externas podrán requerir acceso a logs históricos para verificar el cumplimiento de políticas y procedimientos establecidos.

V. **Normativas de referencia**

Este proceso se alinea completamente con el marco legal aplicable, incluyendo la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los lineamientos de seguridad emitidos por transparencia. Adicionalmente, cumple con las normativas internacionales ISO/IEC 27001:2022, ISO/IEC 27701 e ISO

27035 para gestión de incidentes, así como con las buenas prácticas reconocidas internacionalmente como NIST SP 800-53 y CIS Controls.

CAPÍTULO XXX
DE LA POLÍTICA DE HABILITACIÓN DE REGISTROS RELEVANTES

CIS CONTROL #8: GESTIÓN DE LOGS DE AUDITORÍA.

I. Propósito y Objetivo

En esta política se establece la obligación de habilitar la generación de registros de auditoría en todos los activos tecnológicos de la SESEA. El propósito de esto es garantizar la trazabilidad completa de eventos, facilitar el análisis de incidentes de seguridad y asegurar el cumplimiento de las normativas vigentes en materia de transparencia y rendición de cuentas.

La implementación de esta política permitirá contar con evidencia digital confiable para investigaciones, auditorías y procesos de mejora continua en la gestión de la seguridad de la información institucional.

II. Alcance

Esta política aplica de manera integral a todos los componentes tecnológicos que conforman la infraestructura institucional, abarcando tanto recursos físicos como virtuales y servicios en la nube. Se incluyen los servidores físicos y virtuales que hospedan servicios críticos, las estaciones de trabajo utilizadas por el personal, dispositivos de red como switches, routers y firewalls que con los cuales se gestiona el tráfico de datos.

También comprende las aplicaciones críticas para el funcionamiento institucional y sus bases de datos asociadas, sistemas implementados en modalidades de nube pública, privada o híbrida, sistemas de respaldo y recuperación ante desastres, así como equipos especializados de seguridad como sistemas de detección de intrusos, soluciones antivirus y plataformas de gestión de eventos e información de seguridad.

III. Descripción de la política

Todos los activos tecnológicos de la SESEA deben mantener la generación de registros de auditoría de forma permanente y continua. Esta habilitación debe realizarse desde el momento de la puesta en operación del activo y mantenerse durante todo su ciclo de vida útil.

Los registros de auditoría deben capturar de manera obligatoria los eventos relacionados con inicios y cierres de sesión de usuarios, incluyendo intentos fallidos de autenticación. Se deben registrar todos los errores críticos del sistema y aplicaciones que puedan impactar la disponibilidad o integridad de los servicios, así como cualquier cambio en la configuración de sistemas o modificaciones en los privilegios de acceso de usuarios. Se debe documentar todos los accesos a información clasificada como sensible o confidencial, registrando la identidad del usuario, fecha, hora y tipo de información consultada. Adicionalmente, se deben capturar todos los comandos ejecutados con privilegios administrativos, incluyendo el contexto y el usuario responsable de la ejecución.

Para habilitar la captura de registros en entornos con Windows, se deben activar las auditorías de seguridad utilizando las Directivas de Grupo o la configuración directa desde la Consola de Eventos del sistema. Para sistemas Linux, se debe habilitar el demonio auditd junto con los servicios syslog, journald o rsyslog según corresponda a la distribución específica implementada.

En el caso de los dispositivos de red, se debe configurar Syslog y SNMP traps porque esto permite la centralización de eventos de red críticos. Las aplicaciones deben activar sus mecanismos de logging nativos o configurar la exportación de eventos hacia sistemas SIEM, servidores de logs centralizados o archivos planos debidamente protegidos.

Para servicios en la nube, se debe habilitar CloudTrail en AWS, Audit Logs en Google Cloud Platform, y Azure Monitor o Microsoft Defender en Azure, asegurando la captura completa de eventos de la infraestructura como servicio.

La información contenida en los logs debe tratarse con el nivel de confidencialidad apropiado, implementando controles de acceso que limiten su consulta únicamente a personal autorizado para fines legítimos de auditoría, investigación o análisis de seguridad.

Todos los registros de auditoría generados se deben gestionar conforme a los lineamientos establecidos en la "Política de Conservación y Retención de Registros de Seguridad" institucional. Porque en esta política se garantiza la protección contra alteraciones no autorizadas mediante controles de integridad y almacenamiento en medios confiables y seguros.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital ejerce la supervisión general del cumplimiento de esta política, realizando auditorías periódicas para verificar el estado de habilitación de logs en todos los activos institucionales. Coordinar las revisiones de cumplimiento en alineación con las políticas de seguridad establecidas y actúa como punto de escalamiento para resolver incidencias relacionadas con la gestión de registros de auditoría.

La Dirección de Servicios Tecnológicos debe establecer un programa de revisiones periódicas con frecuencia semestral o anual para evaluar el estado de habilitación de registros en todos los activos tecnológicos. Estas revisiones forman parte integral de las auditorías de cumplimiento del Sistema de Gestión de Seguridad de la Información y deben documentarse adecuadamente para evidenciar el nivel de adherencia a esta política.

Esta unidad también tiene la responsabilidad de verificar que cada nuevo activo tecnológico incorporado a la SESEA cuente con la habilitación de logs antes de su puesta en operación productiva. Debe configurar adecuadamente el almacenamiento de registros, ya sea de forma local o centralizada, considerando la criticidad del activo y los requisitos de disponibilidad.

V. **Normativas de referencia**

Esta política se fundamenta en el cumplimiento de estándares internacionales y normativas nacionales aplicables. Se alinea específicamente con ISO/IEC 27001:2022 en su control A.8.15 referente a registros de eventos de seguridad, NIST SP 800-53 en su control AU-2 sobre eventos auditables, y los requisitos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

CAPÍTULO XXXI

DE LA POLÍTICA PARA ALMACENAR Y PROTEGER LOS REGISTROS DE AUDITORÍA

CIS CONTROL #8: GESTIÓN DE LOGS DE AUDITORÍA.

I. Propósito y Objetivo

En esta política se establecen los lineamientos necesarios para garantizar el almacenamiento confiable, seguro y suficiente de los registros de auditoría generados por los activos tecnológicos de la SESEA. Su finalidad es asegurar la conservación adecuada de estos registros conforme a los tiempos de retención establecidos, manteniendo su integridad y disponibilidad para fines de auditoría, investigación y cumplimiento normativo.

II. Alcance

Esta política aplica a todos los sistemas que generan logs o registros de auditoría dentro de la infraestructura tecnológica de la SESEA. Esto incluye servidores con sistemas operativos Windows y Linux, equipos de red como firewalls, routers y switches, aplicaciones empresariales, plataformas en la nube, y sistemas de respaldo y almacenamiento. La aplicación de esta política es obligatoria para todos los usuarios, administradores y personal técnico que interactúe con estos sistemas.

III. Lineamientos Generales de Almacenamiento

Para almacenar y proteger los registros de auditoría de una manera efectiva, se deben de tomar en consideración, al menos, los criterios de almacenamiento siguientes:

a) **Almacenamiento Local.** Para activos individuales, los logs deberán almacenarse en discos separados del sistema operativo cuando sea técnicamente posible. Esta separación física y/o lógica garantiza que los registros no afecten el rendimiento del sistema principal y se reduzca el riesgo de pérdida por fallos del sistema operativo. Los discos destinados a este propósito deben tener asignado al menos el 20 por ciento de su capacidad total disponible para registros de auditoría, aunque este

porcentaje puede incrementarse según la naturaleza del sistema y el volumen de logs generados;

b) **Almacenamiento Centralizado.** Para aquellos sistemas que manejen información sensible se deben exportar sus logs a un servidor central de logs, esto mediante tecnologías como Syslog, SIEM, Wazuh u otras soluciones similares. Este servidor centralizado debe contar con espacio proyectado para al menos 24 meses de retención, calculado según las tasas promedio de generación de registros. Además, se debe implementar políticas de respaldo y cifrado para proteger la información, así como controles de acceso basados en roles para garantizar que solo el personal autorizado pueda acceder a los registros;

c) **Cifrado y Protección.** Los registros de auditoría deben almacenarse en medios cifrados o protegidos contra escritura y modificación no autorizada. Esta protección es fundamental para mantener la integridad de la evidencia digital y cumplir con los requisitos de auditoría. Cuando sea necesario, se deben aplicar controles adicionales de integridad como funciones hash o firmas digitales que permitan verificar que los registros no han sido alterados desde su creación;

d) **Proyecciones de Capacidad.** La Dirección de Servicios Tecnológicos y Plataforma Digital realizará estimaciones semestrales del volumen de logs generados por todos los sistemas incluidos en el alcance de esta política. Basándose en estas proyecciones, se ajustará la capacidad del almacenamiento para asegurar el cumplimiento del período de retención definido en la Política de Conservación de Registros, que establece períodos de uno a dos años según el tipo de registro y su sensibilidad;

e) **Verificación de espacio.** El área de infraestructura tiene la responsabilidad de verificar al menos mensualmente el uso de disco destinado a logs, analizar las tendencias de crecimiento y monitorear alertas de uso crítico cuando se supere el 80 por ciento de la capacidad disponible. Esta verificación debe documentarse y cualquier anomalía o tendencia preocupante debe escalarse inmediatamente para tomar acciones preventivas.

Los sistemas deben operar bajo un esquema de monitoreo continuo donde se establezcan diferentes niveles de acción según el porcentaje de uso del disco. Cuando el uso se encuentra por debajo del 70 por ciento, se considera operación normal sin requerir acciones adicionales. Entre el 70 por ciento y 85 por ciento se activa una revisión preventiva para evaluar la necesidad de acciones futuras. Al superar el 85 por ciento se requieren acciones inmediatas para evitar la saturación, y cuando se alcanza el 95 por ciento se considera un riesgo crítico de pérdida de logs que requiere escalamiento automático y atención urgente.

Todos los sistemas deben contar con alertas automáticas para notificar al personal responsable cuando se alcancen estos umbrales críticos. Cuando se alcancen niveles críticos, es indispensable ejecutar las siguientes acciones para detectar el origen de la saturación;

f) **Rotación de Logs.** Los archivos antiguos deben comprimirse automáticamente y almacenarse en volúmenes separados o en sistemas NAS para liberar espacio en el almacenamiento primario, manteniendo la disponibilidad de los registros históricos. Algunas herramientas de ayuda con este fin son: en servidores Linux se utiliza logrotate, en sistemas Windows se utiliza Event Log archiving;

g) **Depuración Controlada.** Bajo ninguna circunstancia se deben eliminar logs sin contar previamente con un respaldo adecuado. El proceso de depuración debe seguir un protocolo estricto que incluye la compresión de registros más antiguos, la transferencia a medios externos o servicios en la nube cuando sea aplicable, y el registro detallado de todas las acciones realizadas en una bitácora de depuración que permita la trazabilidad completa del proceso;

h) **Expansión de Almacenamiento.** Cuando el crecimiento del volumen de logs sea sostenido y las medidas de rotación y compresión no sean suficientes, se debe ampliar los volúmenes de disco o asignar almacenamiento adicional. Esta expansión debe estar incluida en el plan de continuidad operativa para garantizar que no se vea comprometida la disponibilidad de los servicios; y,

i) **Registro y Auditoría de Acciones.** Todas las acciones realizadas sobre los logs deben documentarse exhaustivamente en la bitácora técnica correspondiente (Anexo I). Esta documentación debe incluir la fecha y hora de la acción, el responsable que la ejecutó, el motivo específico, los archivos afectados, y el método de resguardo utilizado. Adicionalmente, todas estas acciones deben ser revisadas por la Dirección de Servicios Tecnológicos dentro de las 48 horas siguientes para validar su correcta ejecución y cumplimiento de los procedimientos establecidos.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de monitorear continuamente el espacio y la ejecución de acciones técnicas para resolver situaciones de saturación de logs. También debe validar la conservación e integridad de los registros tras cualquier intervención. Y debe asegurar la disponibilidad de almacenamiento adicional cuando sea necesario y participar en la planificación de expansiones futuras.

CAPÍTULO XXXII
DE LA POLÍTICA DE USO DE NAVEGADORES Y CORREO ELECTRÓNICO

CIS CONTROL #9: PROTECCIÓN DE CORREO ELECTRÓNICO Y NAVEGADOR WEB

I. Propósito y Objetivo

Establecer los lineamientos para el uso de navegadores web y clientes de correo electrónico en la SESEA, garantizando que solo se utilicen versiones compatibles, actualizadas y seguras. Con esta política se busca proteger la información institucional y reducir los riesgos de seguridad mediante el uso exclusivo de herramientas que cuenten con el respaldo oficial de sus proveedores y que reciban actualizaciones regulares de seguridad.

II. Alcance

Esta política aplica a todos los equipos de cómputo que accedan a internet o correo electrónico institucional. Se incluyen las computadoras de escritorio y portátiles asignadas al personal, así como los equipos de cómputo institucional ubicados en salas o áreas comunes. También abarca los sistemas virtualizados o en la nube que requieran acceso a internet o correo electrónico, además de los dispositivos móviles autorizados para el uso de correo institucional.

III. Descripción de la política

El acceso a internet institucional se debe realizar únicamente a través de navegadores oficiales y actualizados que garanticen la seguridad de la información. Los navegadores autorizados incluyen Google Chrome en su última versión estable publicada por Google, Mozilla Firefox en su versión más reciente y estable publicada por Mozilla, Microsoft Edge en su versión más actual basada en Chromium, y Safari exclusivamente en equipos Apple con la última versión publicada por Apple.

Está estrictamente prohibido el uso de navegadores obsoletos o sin soporte técnico continuo. Internet Explorer en cualquiera de sus versiones no debe utilizarse bajo ninguna circunstancia, al igual que navegadores alternativos que no cuenten con

actualizaciones de seguridad constantes o que no sean reconocidos por proveedores oficiales.

Por su parte, el manejo del correo electrónico institucional debe realizarse exclusivamente a través de clientes oficiales y debidamente actualizados. Se autoriza el uso de Google Gmail a través del navegador web, Microsoft Outlook en cualquiera de sus modalidades incluyendo la versión de escritorio, Microsoft 365 o Outlook Web App, Mozilla No se permite bajo ninguna circunstancia el uso de clientes de correo no oficiales desarrollados por terceros, accesos mediante protocolos POP o IMAP que no estén cifrados, ni aplicaciones de correo que carezcan de soporte oficial o que no reciban parches de seguridad regulares.

Todos los navegadores y clientes de correo electrónico deben mantenerse en sus versiones más recientes mediante la activación de sus funciones de actualización automática. Esta medida garantiza que las herramientas cuenten con los últimos parches de seguridad y correcciones de vulnerabilidades.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos tiene la responsabilidad de verificar trimestralmente que todas las versiones del Software instaladas en los equipos institucionales estén dentro de las versiones soportadas oficialmente. Cuando las actualizaciones automáticas no estén habilitadas o no funcionen correctamente, dicha dirección debe aplicar actualizaciones manuales de forma inmediata. Además, debe implementar el bloqueo de versiones obsoletas mediante políticas de grupo o herramientas de gestión de endpoints para prevenir el uso de Software vulnerable.

La instalación de nuevos navegadores o clientes de correo electrónico es una actividad exclusiva de la Dirección de Servicios Tecnológicos, que también tiene la facultad de autorizar excepciones justificadas. Cualquier Software no autorizado que sea detectado en los equipos institucionales será eliminado de manera inmediata, sin excepción.

V. **Normativa de referencia**

Esta política se fundamenta en estándares internacionales de seguridad de la información, específicamente en la norma ISO/IEC 27001:2022 en su control A.8.10

referente a la seguridad de Software de usuario. También se alinea con el Marco de Ciberseguridad del NIST en sus funciones ID.AM-5 y PR.IP-1, incorpora las buenas prácticas de seguridad recomendadas por los proveedores oficiales como Microsoft, Google y Mozilla, y cumple con los requisitos de Ciberhigiene establecidos para el sector público en México.

CAPÍTULO XXXIII

DE LA POLÍTICA DE USO DE SERVICIOS DE FILTRADO DNS PARA BLOQUEO DE DOMINIOS MALICIOSOS

CIS CONTROL #9: PROTECCIÓN DE CORREO ELECTRÓNICO Y NAVEGADOR WEB

I. **Propósito y Objetivo**

En esta política se establece el uso obligatorio de servicios de filtrado DNS en todos los activos tecnológicos de la SESEA. Su propósito fundamental es crear una primera línea de defensa contra amenazas cibernéticas mediante la prevención del acceso a sitios web o dominios maliciosos conocidos. Con esta medida se busca reducir significativamente el riesgo de infecciones por malware, la filtración no autorizada de datos institucionales y los ataques basados en técnicas de phishing o distribución de software malicioso que pueden comprometer la integridad y confidencialidad de la información.

II. **Alcance**

Esta política se aplica a todos los activos de red institucionales que forman parte de la infraestructura tecnológica de la SESEA. Esto incluye las estaciones de trabajo utilizadas por el personal, todos los servidores que prestan servicios para la operación, los dispositivos móviles que han sido autorizados para acceder a recursos institucionales, y los equipos de red que facilitan la conectividad y comunicación. Asimismo, comprende los servicios en la nube que requieren resolución de nombres de dominio desde la red organizacional, para garantizar que toda comunicación digital mantenga los estándares de seguridad establecidos.

III. **Descripción de la política**

Todos los dispositivos que se conecten a la red institucional deben configurarse obligatoriamente para utilizar servicios DNS que cuenten con capacidades avanzadas de filtrado. Estos servicios pueden ser implementados internamente por la SESEA o contratados a proveedores externos que demuestren confiabilidad y efectividad. El sistema de filtrado debe realizar el bloqueo automático de dominios que han sido identificados como asociados a malware, campañas de phishing, redes de botnets, spyware y ransomware. Adicionalmente, deben incorporar dominios

incluidos en listas actualizadas de inteligencia de amenazas que proporcionan información en tiempo real sobre nuevas amenazas emergentes.

Existen DNS que han demostrado eficacia en el filtrado de amenazas, por ende pueden ser implementados en la SESEA, entre estos se encuentran Cisco Umbrella (anteriormente conocido como OpenDNS), Quad9 con su servicio disponible en la dirección 9.9.9.9, Cloudflare Gateway DNS, Google Safe DNS complementado con políticas de firewall apropiadas, y servidores DNS institucionales que cuenten con filtrado integrado. Cualquier otro servicio DNS que se considere para implementación debe ser previamente evaluado y aprobado por la Dirección de Servicios Tecnológicos para garantizar que cumple con los estándares de seguridad requeridos.

Por parte de la configuración del DNS en equipos personales, los usuarios finales deben poder tener acceso de manera forzosa el uso del servicio DNS autorizado, eliminando así la posibilidad de que los usuarios finales realicen modificaciones manuales que puedan comprometer la seguridad. Esta medida garantiza que no se puedan evadir los controles de seguridad mediante la configuración de servidores DNS alternativos que no cuenten con las capacidades de filtrado necesarias.

En el caso de los firewalls y controladores de red institucionales, se deben implementar reglas específicas que redirijan automáticamente todas las solicitudes DNS externas hacia los servicios permitidos y autorizados. Simultáneamente, se deben configurar para bloquear activamente cualquier intento de resolución DNS que se realice a través de servidores no autorizados, manteniendo la integridad del sistema de filtrado establecido.

En situaciones donde un dominio legítimo sea bloqueado incorrectamente por el sistema de filtrado, el área afectada podrá solicitar una exclusión temporal del bloqueo. Esta solicitud debe ser procesada y validada previamente por la Dirección de Servicios Tecnológicos para verificar la legitimidad del dominio y evaluar los riesgos asociados. Todas las excepciones deben ser debidamente documentadas, justificadas técnicamente y establecerse con una vigencia limitada que permita revisiones periódicas de su necesidad.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos tiene la responsabilidad de realizar revisiones trimestrales para verificar que todos los activos tecnológicos estén resolviendo correctamente las consultas DNS a través del servicio autorizado. Estas revisiones también deben confirmar que no se esté utilizando DNS no autorizado mediante métodos como túneles, aplicaciones no controladas o conexiones VPN que evadan los controles institucionales.

V. **Normativas de referencia**

Esta política se fundamenta en estándares internacionales reconocidos que incluyen ISO/IEC 27001:2022 en sus controles A.8.7 referente a la protección contra malware y A.8.23 sobre filtrado web, los CIS Controls v8 específicamente el Control 9 sobre filtrado DNS, y el NIST Cybersecurity Framework en sus funciones PR.DS-1 y PR.PT-4. Adicionalmente, se basa en las mejores prácticas de Ciberhigiene y protección contra amenazas persistentes reconocidas por la comunidad internacional de seguridad cibernética.

CAPÍTULO XXXIV
DE LA POLÍTICA PARA GESTIONAR SOFTWARE ANTIMALWARE

CIS CONTROL #10: DEFENSAS CONTRA MALWARE

I. Propósito y Objetivo

La presente política tiene como finalidad establecer las directrices que se deben seguir en la SESEA en materia de instalación y mantenimiento de Software antimalware en todos los activos tecnológicos de la SESEA. Con este documento se busca salvaguardar la información institucional, los sistemas informáticos y la infraestructura tecnológica de la SESEA contra las diversas amenazas de software malicioso, que incluyen virus informáticos, gusanos, programas troyanos, ransomware, spyware y cualquier otra forma de código malicioso que pueda comprometer la integridad, confidencialidad y disponibilidad de los recursos tecnológicos institucionales.

II. Alcance

La aplicación de esta política abarca la totalidad de los activos tecnológicos que forman parte del ecosistema digital de la SESEA. Esto comprende las computadoras de escritorio utilizadas en las diferentes áreas de trabajo, las laptops asignadas al personal para el desempeño de sus funciones, así como todos los servidores tanto físicos como virtuales que soportan las operaciones críticas de la SESEA. Igualmente, se incluye cualquier otro dispositivo electrónico que se conecte a la red institucional de la SESEA o que sea empleado para acceder, procesar o almacenar información perteneciente a la organización, independientemente de su ubicación física o modalidad de uso.

III. Descripción de la política

Para garantizar una protección efectiva contra amenazas de malware, todos los activos tecnológicos al alcance de esta política deben cumplir con requisitos específicos que aseguren una defensa robusta y actualizada.

En primer lugar, es indispensable que cada activo tecnológico cuente con un software antimalware que haya sido previamente aprobado por la Dirección de Servicios Tecnológicos y Plataforma Digital. Esta instalación debe realizarse de manera correcta y completa antes de que el dispositivo sea conectado a la red institucional o utilizado para acceder a la información de la SESEA. Al conectarse de esta manera se evitan vulnerabilidades durante el proceso de incorporación del equipo al ambiente de trabajo.

Una vez instalado, el Software debe mantenerse constantemente actualizado a través de la configuración de actualizaciones automáticas y periódicas, tanto de las definiciones de virus como del propio programa, asegurando que la protección evolucione al mismo ritmo que las nuevas amenazas.

El sistema de análisis debe operar en dos modalidades complementarias: análisis programados y monitoreo en tiempo real. Los análisis completos del sistema deben ejecutarse de forma regular, con una periodicidad mínima mensual, para realizar una revisión exhaustiva que permita detectar y eliminar cualquier posible infección de malware que haya podido evadir las defensas iniciales. Paralelamente, la protección en tiempo real debe permanecer activa de forma continua, monitoreando activamente el comportamiento del sistema para identificar y neutralizar amenazas en el momento mismo en que se manifiesten.

La configuración del Software antimalware debe ajustarse estrictamente a las directrices establecidas por la Dirección de Servicios Tecnológicos y Plataforma Digital, incluyendo parámetros específicos para los procesos de análisis, cuarentena y eliminación de Software malicioso, asegurando una respuesta homogénea y eficaz ante las amenazas detectadas.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de liderar la estrategia de protección antimalware de la SESEA. Esta Dirección debe llevar a cabo un proceso riguroso de selección, evaluación y aprobación de las soluciones de Software antimalware que se implementarán en toda la organización, considerando aspectos técnicos, económicos y de compatibilidad con la infraestructura existente. Asimismo, le corresponde establecer y ejecutar un programa de monitoreo continuo del cumplimiento de esta política mediante

auditorías periódicas que permitan identificar desviaciones y oportunidades de mejora.

Cuando se presenten incidentes de seguridad relacionados con malware, esta Dirección debe asumir el liderazgo en la investigación y respuesta, coordinando las acciones necesarias para contener la amenaza, evaluar el impacto e implementar las medidas correctivas correspondientes. Adicionalmente, tiene la responsabilidad de asegurar que el Software antimalware de todos los servidores institucionales permanezcan actualizados y funcionando de manera óptima.

El personal de la SESEA que tengan bajo su responsabilidad activos tecnológicos, tienen la responsabilidad de garantizar que todos los dispositivos que utilicen, son para fines laborales y cuenten con la instalación del Software antimalware aprobado institucionalmente y funcionando. También deben mantener estos programas actualizados y ejecutar los análisis periódicos del sistema según las directrices establecidas, siguiendo las configuraciones y procedimientos indicados por la Dirección de Servicios Tecnológicos y Plataforma Digital. Es fundamental que estos usuarios también reporten de inmediato cualquier actividad sospechosa o posible infección de malware que detecten, y bajo ninguna circunstancia deben deshabilitar o manipular el Software antimalware instalado, ya que esto comprometería la seguridad de toda la red institucional.

Las personas titulares de cada unidad tienen la responsabilidad de que todo el personal bajo su responsabilidad cumpla cabalmente con las disposiciones de esta política. Deben verificar regularmente que los activos tecnológicos de su área cuenten con el software antimalware instalado y actualizado, y proporcionar el apoyo necesario a la Dirección de Servicios Tecnológicos y Plataforma Digital para garantizar el cumplimiento efectivo de todas las disposiciones contenidas en el presente Manual.

CAPÍTULO XXXV
DE LA POLÍTICA DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS ANTIMALWARE

CIS CONTROL #10: DEFENSAS CONTRA MALWARE

I. Propósito y Objetivo

La presente política establece la obligación de mantener activadas las actualizaciones automáticas de las firmas de virus, malware y demás amenazas cibernéticas en todos los activos tecnológicos de la SESEA. Con este requisito se busca garantizar una protección continua y efectiva frente a las amenazas emergentes que evolucionan constantemente en el panorama digital, asegurando así que los sistemas que se administran en la SESEA mantengan las defensas más actualizadas disponibles.

II. Alcance

Esta política es de aplicación obligatoria para todos los dispositivos institucionales que cuenten con software antimalware instalado sin excepción. El alcance comprende las estaciones de trabajo que operen bajo sistemas Windows, Linux o macOS, así como todos los servidores físicos o virtuales que formen parte de la infraestructura tecnológica. También incluye equipos portátiles asignados al personal, dispositivos móviles corporativos cuando sea técnicamente aplicable, y máquinas virtuales, junto con sistemas en la nube que se encuentren bajo administración directa de la SESEA.

III. Descripción de la política

Todos los activos tecnológicos que pertenezcan a la SESEA, deben cumplir de manera estricta con los siguientes requisitos. Cada dispositivo debe contar con un software antimalware.

La solución antimalware institucional debe cumplir con características técnicas específicas que garanticen su efectividad y capacidad de gestión. En ambientes con más de 10 equipos, es obligatorio contar con una consola central de administración que permita la gestión unificada de todos los dispositivos. La solución debe ser capaz de generar alertas automáticas en caso de fallos en la actualización,

facilitando la respuesta inmediata ante cualquier problema. Además, debe registrar todos los eventos de actualización en archivos de log. Entre las soluciones aceptadas, según el licenciamiento institucional actual, se encuentran Microsoft Defender for Endpoint, ESET y McAfee.

La función de actualización automática de firmas de virus y malware debe mantenerse habilitada en todo momento, sin permitir su desactivación manual, salvo en casos excepcionales debidamente autorizados. Adicionalmente, es indispensable verificar periódicamente la conectividad con los servidores de actualización del fabricante para asegurar que las actualizaciones se reciban de manera oportuna y sin interrupciones.

Las actualizaciones de firmas deben ejecutarse con una frecuencia mínima de una vez al día, aunque de ser posible, se debe aumentar dicha frecuencia para mejorar la efectividad.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos tiene la responsabilidad de supervisar regularmente el correcto funcionamiento de las actualizaciones automáticas, realizando verificaciones al menos una vez por semana para confirmar que todos los activos estén actualizando correctamente sus firmas de protección. Cualquier error o falla detectada en el proceso de actualización debe ser registrado de manera inmediata en los sistemas de control correspondientes y corregido en un plazo no mayor a 24 horas. Este monitoreo proactivo permite identificar problemas potenciales antes de que comprometan la seguridad de los sistemas institucionales.

V. **Normativas de referencia**

Esta política se fundamenta en estándares internacionales y mejores prácticas reconocidas en el ámbito de la Ciberseguridad. Se alinea con los controles establecidos en ISO/IEC 27001:2022, específicamente el Control A.8.7 relacionado con la protección contra malware. También incorpora los lineamientos del CIS Controls v8, particularmente el Control 10 sobre defensas contra malware, y se basa en las recomendaciones del NIST Cybersecurity Framework, específicamente el control PR.IP-12 para protección frente a software malicioso. Adicionalmente, considera las buenas prácticas de Ciberhigiene promovidas por el Gobierno Federal y los organismos de transparencia, asegurando coherencia con las políticas nacionales de seguridad digital.

CAPÍTULO XXXVI
DE LA POLÍTICA PARA DESACTIVAR AUTORUN Y AUTOPLAY EN MEDIOS EXTRAÍBLES

CIS CONTROL #10: DEFENSAS CONTRA MALWARE

I. **Propósito y Objetivo**

Establecer la directriz de deshabilitar la ejecución automática (AutoRun) y la reproducción automática (AutoPlay) en todos los activos tecnológicos de la SESEA. Con esta medida preventiva se busca evitar la ejecución no autorizada de código malicioso a través de medios extraíbles como memorias USB, discos ópticos (CD/DVD) o discos externos, fortaleciendo así la postura de seguridad institucional ante amenazas cibernéticas que aprovechan estas vulnerabilidades.

II. **Alcance**

Esta política aplica de manera obligatoria a todos los dispositivos institucionales que forman parte de la infraestructura tecnológica de la SESEA, esto incluye computadoras de escritorio y portátiles utilizadas por el personal, así como servidores físicos o virtuales que soportan las operaciones de la organización. La política abarca equipos con sistema operativo Windows, Linux o macOS, sin importar su versión, siempre que cuenten con puertos USB habilitados o lectores ópticos que permitan la conexión de medios extraíbles.

III. **Descripción de la política**

Las funciones AutoRun y AutoPlay han sido históricamente identificadas como vulnerabilidades de ataque preferidas por actores maliciosos para la distribución de amenazas cibernéticas. Estas funciones facilitan la ejecución automática de malware almacenado en memorias USB infectadas, la activación de troyanos ocultos en discos aparentemente legítimos, el despliegue de herramientas de acceso remoto sin autorización del usuario, y la propagación de gusanos que se extienden automáticamente a través de redes locales.

Todos los activos tecnológicos deben cumplir con la desactivación completa de las funciones AutoRun y AutoPlay para garantizar un entorno seguro. La desactivación de AutoRun impide que los archivos configurados para ejecutarse automáticamente

desde medios extraíbles se inician sin la intervención explícita del usuario, eliminando así la posibilidad de ejecución inadvertida de código potencialmente malicioso. De esta manera, la desactivación de AutoPlay impide que el sistema operativo sugiera acciones automáticas como reproducir contenido multimedia, abrir carpetas o instalar software al insertar un medio externo, manteniendo el control total en manos del usuario autorizado.

La implementación de estas configuraciones debe realizarse mediante métodos técnicos apropiados para cada entorno operativo. En entornos Windows, se utilizarán políticas de grupo (GPO). Para máquinas locales o entornos descentralizados, se emplearán scripts de configuración desarrollados en PowerShell para sistemas Windows o Bash para sistemas basados en Unix. Como alternativa complementaria, se pueden realizar ajustes directos en el registro del sistema operativo o mediante la configuración de políticas de seguridad local, asegurando que la implementación sea robusta y permanente.

Esta implementación preventiva asegura que, desde el primer momento de operación, los equipos cuenten con las medidas de protección. Adicionalmente, se deben realizar revisiones periódicas con una frecuencia de seis meses para verificar que la política no haya sido modificada inadvertidamente por el usuario final o por actualizaciones del sistema operativo. Esta validación puede integrarse como parte de las auditorías internas de Ciberhigiene, permitiendo una supervisión continua del cumplimiento de la política.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de garantizar que esta configuración se aplique de manera sistemática durante el proceso de creación de la imagen base o configuración inicial de todos los equipos institucionales.

Cualquier necesidad operativa de habilitar temporalmente las funciones AutoPlay o AutoRun para fines específicos, como la recuperación de sistemas antiguos o la instalación de Software especializado, debe seguir un proceso formal de aprobación. Esta solicitud debe ser evaluada y aprobada por la Dirección de Servicios Tecnológicos, estableciendo una vigencia máxima claramente definida para la excepción. Todas las excepciones autorizadas deben documentarse adecuadamente en el registro de excepciones de seguridad, incluyendo la

justificación técnica, el período de vigencia y las medidas compensatorias implementadas durante la excepción.

V. **Normativa de referencia**

Esta política se fundamenta en estándares internacionales reconocidos de seguridad de la información. Se alinea con los requisitos establecidos en ISO/IEC 27001:2022, específicamente el Control A.8.7 relacionado con la protección contra malware. También cumple con las recomendaciones del CIS Controls v8, particularmente el Control 10.7 que establece la necesidad de deshabilitar AutoRun y AutoPlay. Finalmente, se sustenta en las directrices del NIST SP 800-53 Rev. 5, específicamente el Control SI-3 referente a la auto-ejecución, garantizando que la implementación siga las mejores prácticas reconocidas a nivel internacional.

CAPÍTULO XXXVII
DE LA POLÍTICA ACERCA DEL PROCEDIMIENTO DE RECUPERACIÓN DE DATOS ANTE PÉRDIDA O INCIDENTE

CIS CONTROL #11: RECUPERACIÓN DE DATOS.

I. **Propósito y Objetivo**

En esta política se establece un proceso robusto para la recuperación de datos institucionales cuando se presentan situaciones de pérdida, corrupción o incidentes de seguridad que comprometan la información de la organización. El objetivo principal es restaurar la operación normal de los sistemas con la menor afectación posible al funcionamiento institucional, priorizando siempre los activos críticos para la continuidad de la SESEA y manteniendo la seguridad e integridad de los respaldos durante todo el proceso de recuperación.

II. **Alcance**

Esta política se aplica a todos los componentes tecnológicos y de información que sustentan las operaciones de la SESEA. Su cobertura incluye los sistemas como servidores, bases de datos, correo electrónico institucional y sistemas de almacenamiento. También abarca toda la información almacenada en servidores físicos, virtuales o en servicios de nube. Finalmente, contempla todos los respaldos de información, ya sean generados de manera automática o manual, que forman parte de la estrategia de protección de datos institucionales.

III. **Descripción de la política**

El proceso de recuperación se debe activar cuando se presentan situaciones que comprometen la disponibilidad o integridad de los datos institucionales. En estas situaciones se incluyen fallos de hardware que afecten el funcionamiento de los sistemas, o corrupción de la lógica que impida el acceso normal a la información. También se debe activar ante infecciones por ransomware o malware que cifre o elimine datos delicados, así como errores humanos que resulten en la pérdida accidental de información importante. Este proceso se debe también iniciar cuando se detecta eliminación accidental o deliberada de archivos o bases de datos, y en

casos de incidentes de seguridad o sabotaje interno que afecten la integridad de los sistemas.

Una vez activado el proceso de recuperación, es fundamental realizar una evaluación exhaustiva para determinar qué sistemas y datos fueron afectados por el incidente. Esta evaluación debe establecer el alcance del daño, clasificándose como parcial cuando solo algunos componentes están afectados, o total cuando el sistema completo ha sido comprometido. Para realizar esta evaluación de manera efectiva, se debe consultar el inventario de activos tecnológicos y las clasificaciones de criticidad previamente establecidas, lo que permite priorizar adecuadamente las acciones de recuperación.

La estrategia de recuperación se basa en un esquema de priorización que considera el daño de cada sistema y su impacto. Los sistemas de alta prioridad incluyen servidores de producción, bases de datos institucionales, correo electrónico y el sistema de expediente electrónico, los cuales deben ser restaurados en menos de 8 horas debido a su importancia para las operaciones diarias.

Los sistemas de prioridad media, como aplicaciones secundarias, sitios web institucionales y carpetas compartidas, tienen un tiempo objetivo de recuperación de menos de 24 horas, permitiendo cierta flexibilidad sin comprometer significativamente la operación. Finalmente, los sistemas de baja prioridad, que incluyen estaciones de trabajo individuales, archivos personales y archivos archivados, pueden ser restaurados en menos de 48 horas o durante el siguiente día hábil, según la disponibilidad de recursos y la urgencia operativa.

El proceso de recuperación sigue una secuencia estructurada que inicia con la detección del incidente, ya sea a través de reportes de usuarios, sistemas de monitoreo automatizado o auditorías de seguridad. Una vez detectado el problema, se procede a la verificación del alcance real del daño y se determina el tiempo transcurrido desde la última copia de seguridad válida, información crucial para planificar la recuperación.

Posteriormente, se requiere la aprobación del procedimiento de restauración por parte de la Secretaría Técnica, asegurando que se comprenda el impacto y las implicaciones del proceso. La fase de recuperación implica seleccionar el respaldo más reciente que esté libre de corrupción, restaurar la información en un ambiente

seguro o replicado cuando sea posible, y validar la integridad de los datos una vez completada la restauración.

Finalmente, se documenta completamente el incidente, incluyendo los tiempos de respuesta, los responsables involucrados y las evidencias del proceso, creando un registro que servirá para mejorar los procedimientos futuros y cumplir con los requisitos de auditoría.

Para que la recuperación sea más rápida, se debe considerar implementar las medidas a los datos siguientes:

a) **Protección física y software.** Los respaldos de información se deben almacenar en medios que cuentan con protección tanto física como de Software para garantizar su integridad y disponibilidad. Esto incluye servidores separados de los sistemas de producción o almacenamiento en servicios de nube que implementan cifrado robusto. La ubicación física de los respaldos se mantiene en espacios seguros como salas técnicas especializadas o sistemas de almacenamiento en red (NAS) con acceso físico restringido. El acceso a los respaldos debe estar limitado exclusivamente al personal autorizado de la Dirección de Servicios Tecnológicos y Plataforma Digital, mediante controles de acceso rigurosos;

b) **Cifrados.** Todos los respaldos deben implementar cifrado para proteger la información almacenada contra accesos no autorizados. Cuando los respaldos se transportan a ubicaciones externas o se almacenan en servicios de nube, también deben contar con cifrado en tránsito utilizando protocolos seguros como TLS/SSL. Esta doble capa de cifrado asegura que la información permanezca protegida durante todo su ciclo de vida;

c) **Resistencia ante alteraciones.** Los respaldos deben estar protegidos contra eliminación o modificación no autorizada mediante la implementación de controles de acceso basados en roles, la cual limita las operaciones que cada usuario puede realizar. Adicionalmente, se deben implementar versiones o respaldos alternos cuando existe el almacenamiento suficiente, para asegurar que las copias de seguridad no puedan ser alteradas una vez creadas. La verificación periódica de

integridad mediante hashes o validaciones automáticas garantiza que los respaldos mantengan su integridad a lo largo del tiempo; y,

d) **Pruebas de recuperación.** La efectividad del proceso de recuperación se debe validar mediante pruebas de restauración al menos cada tres meses. Esto se debe a que estas pruebas permiten verificar que los procedimientos funcionan correctamente. Los resultados de cada prueba se deben documentar detalladamente, y cuando se identifican fallas o áreas de mejora, se deben actualizarlos procedimientos técnicos correspondientes para garantizar la efectividad del proceso.

IV. Responsabilidades

La Dirección de Servicios Tecnológicos y Plataforma Digital, tiene la responsabilidad de ejecutar los respaldos de información, gestionar los procesos de restauración y mantener actualizada toda la documentación relacionada con estos procedimientos. También supervisar la implementación de las medidas de seguridad establecidas y validar periódicamente la integridad de los respaldos para asegurar su efectividad.
La Secretaría Técnica tiene la responsabilidad de asignar los recursos humanos y tecnológicos que sean requeridos a la Dirección de Servicios Tecnológicos para que dichos controles puedan ser implementados satisfactoriamente.

V. Normativa de referencia

Esta política se fundamenta en estándares internacionales reconocidos para garantizar las mejores prácticas en gestión de respaldos y recuperación de datos. Se basa en ISO/IEC 27001:2022, específicamente en los controles A.8.13 relacionados con copias de seguridad y A.17.1 sobre continuidad del negocio. También incorpora las directrices del NIST SP 800-34 para planificación de contingencias y los controles CIS Controls v8, particularmente el Control 11 sobre recuperación de datos, asegurando un enfoque integral y alineado con las mejores prácticas internacionales.

CAPÍTULO XXXVIII
DE LA POLÍTICA PARA CREAR COPIAS DE SEGURIDAD AUTOMÁTICAS

CIS CONTROL #11: RECUPERACIÓN DE DATOS.

I. **Propósito y Objetivo**

Las copias de seguridad constituyen una línea de defensa esencial, mediante la cual se asegura la recuperación de sistemas informáticos en el menor tiempo posible.

En esta política se establece la obligación de implementar y mantener un sistema robusto de copias de seguridad automáticas para todos los datos de la SESEA. El propósito de esta política es garantizar la protección continua de la información contra pérdidas accidentales, corrupciones de datos o incidentes de seguridad que puedan comprometer la integridad y disponibilidad los sistemas informáticos que se administran en la SESEA.

II. **Alcance**

Esta política abarca todos los activos tecnológicos de la SESEA, sin excepción. Su aplicación se extiende a la infraestructura completa de tecnologías de información que soporta las operaciones diarias de la SESEA.

Los servidores de bases de datos, aplicaciones, sistemas de correo electrónico e infraestructura interna forman el núcleo de los activos tecnológicos. Estos sistemas almacenan y procesan información vital para el funcionamiento institucional, por lo que requieren protección especial mediante respaldos regulares y confiables.

Las computadoras de escritorio del personal que labora en la SESEA tanto de base o por honorarios, también están incluidas en el alcance, reconociendo que estos equipos contienen información valiosa y documentos de trabajo que contribuyen significativamente a las operaciones diarias. La pérdida de esta información podría impactar negativamente la productividad y continuidad operativa.

Todos los sistemas de almacenamiento, ya sean servicios en la nube, servidores virtuales o infraestructura física, deben cumplir con los lineamientos establecidos.

Esto incluye datos sensibles como información financiera, datos personales, documentos legales, registros administrativos y cualquier otra información clasificada como crítica para las operaciones institucionales.

III. **Descripción de la política**

Para realizar copias de seguridad de una manera efectiva, se deben de tomar en consideración, al menos, los puntos siguientes:

a) **Frecuencia de las Copias de Seguridad.** Establecer la frecuencia de respaldo según la sensibilidad de los datos, esto con el fin de optimizar recursos de cómputo mientras, se garantiza protección adecuada. Los sistemas de producción requieren respaldos diarios o continuos cuando sea técnicamente posible, dado que almacenan y procesan información esencial para las operaciones diarias.

Los datos sensibles que incluyen información legal, financiera o personal requieren respaldos diarios o semanales, dependiendo de la frecuencia de actualización y el impacto potencial de su pérdida. Los archivos financieros y datos personales sensibles necesitan esta protección reforzada para cumplir con obligaciones legales y normativas.

Los sistemas secundarios pueden respaldarse semanalmente, ya que su pérdida temporal no afecta significativamente las operaciones principales. Las aplicaciones auxiliares y archivos de trabajo general entran en esta categoría.

Los datos de usuarios finales requieren respaldos semanales para proteger su trabajo individual y documentos locales que contribuyen al funcionamiento institucional. Esta frecuencia es suficiente para la mayoría de archivos personales de usuarios clave, considerando que los documentos críticos generalmente se almacenan en sistemas centralizados;

b) **Tipos de Copias de Seguridad.** La estrategia de respaldo debe de contemplar tres tipos de copias de seguridad para optimizar el uso de recursos y garantizar recuperación eficiente. Las copias completas constituyen la base del sistema de respaldo, ejecutándose

mensualmente para crear un punto de referencia integral de todos los datos críticos y sistemas. Con este tipo de respaldo total se obtiene una línea base sólida desde la cual se pueden realizar restauraciones completas del sistema.

Las copias incrementales complementan la estrategia al respaldar únicamente los datos modificados desde el último respaldo de cualquier tipo. Esta aproximación eficiente se ejecuta semanalmente o con mayor frecuencia según las características específicas de cada sistema, minimizando el tiempo de respaldo y el uso de almacenamiento mientras mantiene la protección actualizada.

Las copias diferenciales capturan todos los cambios realizados desde la última copia completa, se pueden ejecutar de manera semanal, esto para proporcionar un punto intermedio de recuperación. Con este enfoque se facilita la restauración porque, solo se necesita la copia completa más reciente y la copia diferencial correspondiente;

c) **Métodos de Copia de Seguridad.** La implementación de respaldos automatizados constituye un requisito fundamental para garantizar consistencia y confiabilidad. Las herramientas especializadas como Veeam, Acronis, junto con soluciones nativas de nube como AWS Backup y Azure Backup, proporcionan la automatización necesaria para ejecutar respaldos sin intervención manual constante. Estas soluciones también incluyen capacidades de programación avanzada y monitoreo que mejoran la confiabilidad del proceso.

El almacenamiento seguro de los respaldos requiere ubicaciones protegidas que incluyen almacenamiento en red dedicado y servicios de nube especializados. Estas ubicaciones deben implementar controles de acceso rigurosos para prevenir accesos no autorizados, garantizando así que los respaldos permanezcan íntegros y disponibles únicamente para personal autorizado;

d) **Seguridad de las Copias de Seguridad.** Al realizar una copia, de seguridad, dicha copia debe de ajustarse a ciertas operaciones, como lo es el cifrado, restringir acceso no autorizado y que sea recuperable, como se detalla a continuación:

1. **Cifrado de Respaldo:** Todas las copias de seguridad deben implementar cifrado robusto tanto durante la transmisión como en el almacenamiento final. El cifrado en tránsito protege los datos mientras se transfieren desde los sistemas origen hacia las ubicaciones de respaldo, utilizando protocolos seguros que previenen intercepción o manipulación durante el proceso de copia.

   El cifrado en reposo garantiza que los datos almacenados permanezcan inaccesibles sin las credenciales de descifrado apropiadas. Esta protección es esencial para cumplir con requisitos de privacidad y seguridad, especialmente cuando los respaldos se almacenan en servicios de terceros o ubicaciones externas;

2. **Acceso Restringido:** El acceso a las copias de seguridad debe limitarse mediante la implementación de controles de acceso basados en roles.

   La autenticación multifactor (MFA) constituye un requisito obligatorio para todos los sistemas de respaldo, añadiendo una capa adicional de seguridad que reduce significativamente el riesgo de accesos no autorizados. Esta medida es especialmente importante considerando la naturaleza sensible de la información contenida en los respaldos;

3. **Pruebas de Recuperación:** Las pruebas de restauración deben ejecutarse al menos mensualmente para verificar la integridad de los respaldos y validar la efectividad de los procedimientos de recuperación. Estas pruebas no solo confirman que los datos se han respaldado correctamente, sino que también aseguran que el personal conoce y puede ejecutar los procedimientos de recuperación cuando sea necesario.

   El proceso de pruebas debe documentarse detalladamente, incluyendo los resultados obtenidos, tiempos de recuperación y cualquier problema identificado durante el proceso. Esta documentación proporciona evidencia del cumplimiento de la política y facilita la mejora continua de los procedimientos; y,

e) **Monitoreo y Auditoría.** Los procesos de respaldo requieren monitoreo continuo y registro detallado en sistemas de auditoría especializados. Esta supervisión garantiza que todos los respaldos se completen correctamente y dentro de los tiempos establecidos.

El sistema que realice copias automáticas, debe generar también alertas automáticas cuando se detecten fallos de respaldo, inconsistencias en los archivos o cualquier anomalía en el proceso. Estas alertas permiten respuesta inmediata a problemas potenciales, minimizando el riesgo de pérdida de protección de datos.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital asume la responsabilidad principal de supervisar y asegurar el cumplimiento integral de esta política. Sus funciones incluyen la realización de auditorías periódicas de los procesos de respaldo, la evaluación de la efectividad de las medidas implementadas y la identificación de oportunidades de mejora en la protección de datos. Adicionalmente, la Dirección de Servicios Tecnológicos tiene la responsabilidad de configurar y mantener las herramientas de respaldo automatizado, garantizando que funcionen correctamente y proporcionen la protección requerida. Esta función incluye la gestión de la infraestructura de respaldo, la implementación de actualizaciones de seguridad y la garantía de accesibilidad de los respaldos cuando sea necesario.

V. **Normativa de referencia**

Esta política se fundamenta en estándares internacionales reconocidos que proporcionan las mejores prácticas en gestión de seguridad de la información y protección de datos. La norma ISO/IEC 27001:2022 en su Control A.8.3 establece los requisitos para la protección de información en caso de pérdida de datos, proporciona el marco conceptual para la implementación de controles de respaldo. Los CIS Controls v8 en su Control 11 sobre Recuperación de Datos ofrecen directrices específicas para la implementación de sistemas de respaldo efectivos. Finalmente, NIST SP 800-53 Rev. 5 en su Control CP-9 que trata de Respaldo de Datos, proporciona controles detallados para la protección y recuperación de información crítica, complementando el marco normativo que sustenta esta política.

CAPÍTULO XXXIX
DE LA POLÍTICA PARA ALMACENAR RESPALDOS DE DATOS

CIS CONTROL #11: RECUPERACIÓN DE DATOS.

I. Propósito y Objetivo

En esta política se establecen los criterios básicos para almacenar respaldos de datos, esto con el objeto de garantizar su integridad, confidencialidad y disponibilidad. La implementación de esta medida incluye el uso de cifrado robusto, sistemas de acceso controlado y, cuando las circunstancias lo requieran, la separación tanto lógica como física de los datos. Estos controles se deben aplicar considerando el nivel de sensibilidad de la información y los requisitos específicos establecidos por la SESEA, asegurando así que los respaldos mantengan el mismo nivel de protección que los datos en producción.

II. Alcance

Esta política se aplica a todos los procesos de respaldo de información que se realicen dentro de la SESEA. Su cobertura incluye los respaldos de bases de datos que contienen información operativa y estratégica, así como los respaldos de aplicaciones esenciales para el funcionamiento de la organización. También abarca los respaldos de archivos y sistemas de información que manejan datos sensibles o confidenciales, independientemente de si estos respaldos se almacenan en medios físicos tradicionales, como cintas o discos duros, o en soluciones de almacenamiento en la nube. Esta política garantiza que todos los tipos de respaldo reciban la protección adecuada sin excepciones.

III. Descripción de la política

Los criterios mínimos que se deben considerar para mantener la seguridad en los respaldos, son:

a) **Acceso Controlado.** Los respaldos deben estar protegidos mediante sistemas de control de acceso estrictos que garanticen que únicamente el personal autorizado pueda acceder a esta información crítica. El acceso estará limitado a roles específicos como administradores de

sistemas certificados y personal especializado de seguridad de la Dirección de Servicios Tecnológicos que hayan sido previamente autorizados y capacitados para estas funciones. La implementación incluirá autenticación multifactor obligatoria y sistemas de control de acceso basado en roles para todas las plataformas de respaldo.

Todos los intentos de acceso a los respaldos, tanto exitosos como fallidos, deben ser registrados automáticamente en un sistema de auditoría que permita detectar cualquier intento no autorizado de acceso. Estos registros incluirán información detallada sobre el usuario, la fecha, hora y tipo de acceso realizado, creando así un rastro de auditoría completo y verificable;

b) **Cifrado de Respaldos.** La protección de los datos de respaldo mediante cifrado es fundamental para mantener la confidencialidad e integridad de la información. Todos los datos de respaldo deben ser cifrados en cuanto sean almacenados (en reposo), como durante su transferencia (en tránsito). El cifrado en reposo debe implementarse utilizando algoritmos robustos como AES-256, reconocido internacionalmente por su fortaleza criptográfica.

Durante la transferencia de datos, se debe utilizar protocolos de seguridad como TLS (Transport Layer Security) para garantizar que la información permanezca protegida mientras se mueve entre sistemas. La gestión de las claves de cifrado debe seguir estrictamente las políticas de seguridad de claves establecidas por la organización, incluyendo procedimientos para la generación, almacenamiento, rotación y destrucción segura de las claves criptográficas;

c) **Separación Lógica o Física.** La separación de los datos de respaldo se utiliza para minimizar los riesgos de seguridad. Cuando los respaldos se almacenan en el mismo entorno de red que los datos originales, debe implementarse una separación lógica efectiva mediante contenedores lógicos independientes, como unidades de almacenamiento virtualizadas con controles de acceso específicos.

Siempre que sea técnica y económicamente viable, los respaldos deben almacenarse en entornos físicos completamente separados o en

ubicaciones remotas. Esta separación física ayuda a mitigar significativamente el riesgo de que los respaldos se vean comprometidos por incidentes que afecten los sistemas de producción, como desastres naturales, ataques cibernéticos o fallas de infraestructura.

Los medios de respaldo físicos requieren almacenamiento en instalaciones especializadas que cuenten con medidas de seguridad física robustas, incluyendo acceso restringido mediante sistemas de control biométrico o tarjetas de acceso, y monitoreo constante las 24 horas. Cuando se utilicen soluciones en la nube, los proveedores de servicios deben demostrar cumplimiento con estándares de seguridad equivalentes o superiores a los implementados en la infraestructura interna de la organización;

d) **Integridad de los respaldos.** La verificación regular de la integridad de los respaldos es esencial para garantizar que los procesos de respaldo se han ejecutado correctamente y que los datos no han sufrido alteraciones o daños. Estas verificaciones deben incluir la generación y comparación de checksums o hashes criptográficos que permitan detectar cualquier modificación no autorizada en los datos.

Se deben establecer procedimientos para realizar pruebas de restauración periódicas que confirmen que los datos de respaldo son completamente accesibles y que el proceso de recuperación funciona correctamente. Estas pruebas deben documentarse y sus resultados deben revisarse regularmente para identificar y corregir cualquier problema potencial antes de que sea necesario usar los respaldos en una situación real.

Los datos clasificados como sensibles, incluyendo información personal, financiera o legal, requieren medidas de protección adicionales que van más allá de los controles estándar. Estos datos deben cifrarse utilizando algoritmos avanzados y pueden requerir implementación de esquemas de cifrado multicapa o duplicación de claves para aumentar la seguridad.

El acceso a respaldos de datos sensibles debe limitarse exclusivamente a personal autorizado que haya recibido capacitación específica sobre el manejo de información confidencial y que cuente con las credenciales de

seguridad apropiadas. El almacenamiento de estos respaldos debe realizarse en servidores dedicados o entornos de nube privados que ofrezcan los más altos niveles de seguridad disponibles, incluyendo controles de acceso físico y lógico reforzados; y,

e) **Monitoreo y Auditoría.** Los procesos de respaldo y todos los accesos a los datos respaldados deben ser monitoreados continuamente en tiempo real mediante sistemas automatizados de detección de amenazas. Cualquier intento de acceso no autorizado o actividad que se considere sospechosa debe generar alertas automáticas que sean inmediatamente escaladas al personal de la Dirección de Servicios Tecnológicos para su revisión e investigación.

   Se debe mantener un registro de auditoría y detallado que incluya información precisa sobre la fecha y hora de cada acceso, la identificación del usuario o entidad que realizó el acceso, las acciones específicas que se llevaron a cabo y cualquier anomalía o comportamiento inusual que haya sido detectado por los sistemas de monitoreo. Estos registros deben conservarse según los requisitos legales y regulatorios aplicables.

IV. Responsabilidades

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad de supervisar la implementación efectiva de esta política en toda la organización y realizar auditorías periódicas de seguridad para verificar el cumplimiento. También debe coordinar la respuesta a incidentes relacionados con los respaldos y mantener actualizados los procedimientos de seguridad.

Esta Dirección, también es responsable de la configuración técnica y el mantenimiento continuo de todos los controles de acceso, sistemas de cifrado e infraestructura de almacenamiento seguro de los respaldos. Debe asegurar que los sistemas funcionen correctamente e implementar las actualizaciones de seguridad necesarias.

V. Normativa de referencia

Esta política se fundamenta en los siguientes estándares y marcos normativos internacionales: ISO/IEC 27001:2022 específicamente en el Control A.8.3 el cual establece los requisitos para la protección de la información en caso de pérdida de datos, NIST SP 800-53 Rev. 5 en su Control CP-9 el cual define los controles para respaldo de datos, y CIS Controls v8 en su Control 11 el cual aborda los aspectos de recuperación de datos. Estos marcos proporcionan las mejores prácticas internacionales para la gestión segura de respaldos de datos.

CAPÍTULO XL
DE LA POLÍTICA DE AISLAMIENTO DE RESPALDO DE DATOS

CIS CONTROL #11: RECUPERACIÓN DE DATOS.

I. **Propósito y Objetivo**

En esta política de la SESEA se establece la necesidad de mantener una instancia completamente aislada de respaldo de datos, esto como medida preventiva ante posibles incidentes de seguridad. El objetivo de esta política busca garantizar la disponibilidad y recuperabilidad de la información institucional, cuando los sistemas de producción y respaldos primarios se vean comprometidos por ciberataques, fallas técnicas o desastres naturales.

Con esta política se busca minimizar significativamente el impacto operacional derivado de la pérdida de datos, permitiendo una reanudación eficiente y oportuna de las operaciones institucionales. La implementación de esta medida fortalece la continuidad y protege la integridad de los procesos anticorrupción que desarrolla la SESEA.

II. **Alcance**

Esta política aplica a la totalidad de los datos, sistemas e infraestructuras necesarias para el funcionamiento operacional de la SESEA. Este alcance incluye las bases de datos institucionales, así como todas las aplicaciones y sus archivos asociados que soportan las operaciones diarias, los sistemas operativos junto con sus configuraciones, y los datos de usuarios que acceden a los sistemas que conforman la Plataforma Digital Estatal.

Adicionalmente, esta política cubre los registros que documentan las actividades realizadas en los sistemas, las comunicaciones electrónicas incluyendo correo electrónico y otras plataformas de mensajería institucional, así como todos los documentos y archivos digitales que forman parte del acervo documental de la SESEA, y cualquier otra información que sea formalmente designada como esencial para el cumplimiento de las funciones institucionales.

III. **Descripción de la política**

La SESEA debe implementar una instancia aislada de datos de recuperación mediante la aplicación estratégica y coordinada de múltiples enfoques de protección. Esta implementación se fundamenta en la combinación de las siguientes estrategias complementarias:

a) **Destinos de Respaldo de Control de Versiones.** La SESEA debe crear un sistema de respaldos semanales con control granular de versiones, lo que significa que cada respaldo constituirá una versión independiente y recuperable de los datos sin sobrescribir versiones anteriores. Este enfoque permite la recuperación precisa a cualquier punto específico en el tiempo, proporcionando flexibilidad excepcional para responder a incidentes de corrupción de datos o ataques de ransomware que puedan haber pasado desapercibidos durante períodos prolongados.

   Estos respaldos versionados se almacenarán en un sistema completamente aislado del entorno de producción, implementando controles de acceso multicapa y mecanismos de autenticación robustos que impidan modificaciones o eliminaciones no autorizadas. La arquitectura de almacenamiento garantizará que los datos de respaldo mantengan su integridad y disponibilidad a lo largo del tiempo;

b) **Sistemas o Servicios Fuera de Línea.** Se debe crear un protocolo para crear copias de seguridad físicas que se almacenarán en medios extraíbles, incluyendo cintas magnéticas de alta capacidad y discos duros externos de grado militar. Estos medios permanecerán completamente desconectados del sistema de producción y de cualquier infraestructura de red, eliminando la posibilidad de acceso remoto.

   El almacenamiento de estos medios se realizará en instalaciones seguras con controles ambientales apropiados, y únicamente se conectarán a sistemas aislados cuando sea estrictamente necesario para procedimientos de recuperación de datos. Se mantendrá un registro meticuloso de todos los medios de respaldo fuera de línea, documentando fechas de creación, contenido específico, fechas de almacenamiento y cualquier actividad de acceso o manipulación;

c) **Almacenamiento en la Nube Segura.** La SESEA debe utilizar servicios de almacenamiento en la nube que cumplan rigurosamente con los estándares de seguridad institucionales y las regulaciones aplicables. Esto implica la implementación de cifrado de extremo a extremo para datos en tránsito y en reposo, controles de acceso granulares basados en roles y responsabilidades específicas, autenticación multifactor obligatoria para todos los accesos, y cumplimiento verificable de las regulaciones de protección de datos y privacidad aplicables.

La selección de proveedores de nube se basará en evaluaciones exhaustivas de seguridad, disponibilidad geográfica y capacidad de respuesta ante incidentes. Se establecerán acuerdos de nivel de servicio que garanticen la disponibilidad y recuperabilidad de los datos bajo cualquier circunstancia; y,

d) **Ubicación Fuera del Sitio.** Se establecerá una ubicación de recuperación de datos que mantenga separación física significativa del centro de datos de producción principal, preferiblemente en una zona geográfica distinta para minimizar el riesgo de desastres simultáneos. Esta ubicación albergará una copia completa de los datos críticos y la infraestructura tecnológica necesaria para restaurar las operaciones esenciales en caso de un desastre que afecte el sitio principal.

La instalación fuera del sitio contará con sistemas de energía redundante, conectividad de comunicaciones independiente y personal técnico capacitado para ejecutar procedimientos de recuperación de manera eficiente y segura.

Además de estas, es recomendable incorporar:

a) **Aislamiento de la Red.** La instancia de recuperación de datos debe mantener aislamiento completo de la red de producción mediante la implementación de segmentación de red física y lógica. Este aislamiento previene la propagación de Malware, ataques laterales y cualquier forma de compromiso que pueda extenderse desde los sistemas de producción hacia los sistemas de recuperación;

b) **Control de Acceso Estricto.** El acceso a la instancia de recuperación de datos estará limitado exclusivamente al personal autorizado mediante la implementación de controles de autenticación multifactor, sistemas de autorización basados en roles mínimos necesarios, y monitoreo continuo de todas las actividades de acceso. Se establecerán procedimientos formales para la concesión, modificación y revocación de permisos de acceso;

c) **Pruebas Periódicas.** Se ejecutarán pruebas sistemáticas y documentadas de la instancia de recuperación de datos con frecuencia trimestral para verificar la integridad de los datos almacenados y la efectividad de los procedimientos de recuperación. Estas pruebas incluirán simulacros de recuperación completa y parcial, validación de la integridad de los datos y verificación de los tiempos de recuperación establecidos;

d) **Documentación.** Todos los procedimientos relacionados con la creación, mantenimiento, prueba y actualización de la instancia de recuperación de datos estarán completamente documentados mediante manuales técnicos, diagramas de arquitectura actualizados y procedimientos operativos estándar. Esta documentación se mantendrá actualizada y accesible para el personal autorizado; y,

e) **Encriptación.** Todos los datos almacenados en la instancia de recuperación estarán protegidos mediante algoritmos de encriptación robustos y actualizados, tanto en reposo como en tránsito. Se implementará gestión segura de claves de encriptación con rotación periódica y almacenamiento seguro de las claves maestras.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital tiene la responsabilidad principal de diseñar, implementar y mantener la instancia aislada de recuperación de datos conforme a las mejores prácticas y los estándares de seguridad institucionales. Dicha dirección debe desarrollar y documentar exhaustivamente los procedimientos de respaldo y recuperación, asegurando que estos sean comprensibles y ejecutables por el personal técnico autorizado.

Esta Dirección debe realizar pruebas periódicas de la instancia de recuperación de datos, documentando los resultados e implementando mejoras continúas basadas en los hallazgos. Debe garantizar la seguridad e integridad de los datos almacenados mediante la implementación de controles técnicos y administrativos apropiados, manteniéndose actualizada con las mejores prácticas y tecnologías emergentes en recuperación de datos.

Adicionalmente, esta Dirección debe configurar y mantener los sistemas de acuerdo con los procedimientos establecidos, informar oportunamente cualquier problema o inquietud relacionado con la instancia de recuperación de datos, e identificar los datos críticos dentro de su área de responsabilidad que deben incluirse en la instancia de recuperación de datos.

Es responsabilidad de todo el personal de la SESEA, ya sea de base o por honorarios, reportar cualquier anomalía o incidente que pueda afectar la integridad de los datos.

CAPÍTULO XLI

DE LA POLÍTICA ACERCA DE LOS DISPOSITIVOS DE RED QUE DEBEN EJECUTAR LA ÚLTIMA VERSIÓN ESTABLE Y COMPATIBLE DEL FIRMWARE/SOFTWARE

CIS CONTROL #12: GESTIÓN DE INFRAESTRUCTURA DE RED.

I. **Propósito y Objetivo**

En este documento se establecen las directrices que la SESEA debe seguir para garantizar que todos los dispositivos de red operen con la versión más reciente, estable y compatible de firmware o Software disponible. El propósito fundamental de esta política es crear un entorno seguro y confiable, donde se minimicen las vulnerabilidades de seguridad informática y se mejore la estabilidad operativa de la infraestructura de red.

La implementación efectiva de esta política contribuye directamente a la protección de la información sensible que maneja la SESEA, y reduce los riesgos de ciberataques.

II. **Alcance**

El alcance de esta política es todos los dispositivos de red que sean propiedad de la SESEA o que estén bajo su administración y control operativo. Esto incluye equipos de infraestructura de red tales como routers que direccionan el tráfico de datos, switches que facilitan la conectividad entre dispositivos; firewalls que protegen el perímetro de la red; puntos de acceso que proporcionan conectividad WiFi; balanceadores de carga que distribuyen el tráfico entre servidores; sistemas de detección y prevención de intrusiones que monitorean amenazas de seguridad; servidores proxy que filtran y controlan el acceso a internet, y cualquier otro dispositivo tecnológico que desempeñe un papel fundamental en la conectividad de red, para garantizar la seguridad de la infraestructura tecnológica institucional.

Esta política también aplica a los dispositivos de red que puedan ser incorporados en el futuro como parte de la expansión o modernización de la infraestructura tecnológica de la SESEA.

III. **Descripción de la Política**

La SESEA establece que todos los dispositivos de red comprendidos en el alcance de esta política deben cumplir con requisitos específicos para garantizar su operación segura y eficiente. Los dispositivos deben ejecutar exclusivamente la versión más reciente y estable del firmware o Software que sea completamente compatible con las especificaciones técnicas del hardware del dispositivo, evitando versiones beta o experimentales que puedan comprometer la estabilidad del sistema.

Antes de proceder con cualquier actualización, es fundamental verificar minuciosamente la compatibilidad del nuevo firmware o Software con el hardware del dispositivo específico y con los demás sistemas de red interconectados, asegurando que no se produzcan interrupciones del servicio o problemas de funcionalidad que puedan afectar las operaciones críticas de la SESEA.

La planificación estratégica de las actualizaciones constituye un elemento esencial para minimizar el impacto en las operaciones diarias de la red institucional. Las actualizaciones que requieran tiempo de inactividad del sistema deben programarse cuidadosamente durante las ventanas de mantenimiento previamente designadas, coordinando con las diferentes áreas usuarias para minimizar las afectaciones a las actividades operativas. Siempre que las condiciones técnicas lo permitan, las actualizaciones de firmware o Software deben someterse a pruebas exhaustivas en un entorno de laboratorio o ambiente de prueba que replique las condiciones de la red de producción. Este proceso de prueba permite identificar y resolver proactivamente cualquier problema potencial, incompatibilidad o conflicto que pueda surgir antes de que afecte negativamente a los sistemas críticos en producción.

Antes de ejecutar cualquier actualización, debe realizarse obligatoriamente una copia de seguridad completa de la configuración actual del dispositivo, incluyendo todos los parámetros de configuración, reglas de seguridad, y ajustes personalizados. Esta copia de seguridad facilita la reversión rápida y segura a la configuración anterior en caso de que la actualización genere problemas o incompatibilidades imprevistas.

Las actualizaciones de seguridad que aborden vulnerabilidades catalogadas como críticas o de alto riesgo deben implementarse de manera prioritaria y oportuna,

siguiendo un proceso acelerado de gestión de parches que permita reducir rápidamente la exposición a amenazas de seguridad, sin comprometer la estabilidad del sistema.

La documentación completa y detallada de todas las actualizaciones es un requisito fundamental para el control y seguimiento de los cambios realizados en la infraestructura. Esta documentación debe incluir información específica sobre la versión de firmware o Software instalada, la fecha exacta de la actualización, el personal técnico involucrado en el proceso, los procedimientos seguidos, y cualquier problema, incidencia o cambio de configuración que haya sido necesario implementar durante el proceso.

El firmware o Software de los dispositivos de red debe contar con soporte activo del fabricante o proveedor para garantizar la disponibilidad continua de actualizaciones de seguridad, parches correctivos y soporte técnico especializado cuando sea requerido. Los dispositivos que hayan perdido el soporte del fabricante deben ser evaluados para su reemplazo o actualización.

Se debe mantener un inventario actualizado y preciso de todos los dispositivos de red, incluyendo información detallada sobre el modelo específico, número de serie, versión actual del firmware o Software, fecha de la última actualización, y estado de soporte del fabricante.

IV. **Responsabilidades**

La Dirección de Servicios Tecnológicos y Plataforma Digital debe establecer y mantener un proceso estandarizado para la gestión de actualizaciones de firmware y Software en todos los dispositivos de red institucionales. Este proceso debe incluir el desarrollo de procedimientos con criterios de evaluación técnica, metodologías de prueba y protocolos de implementación que aseguren la seguridad y continuidad operativa.

La Dirección de Servicios Tecnológicos tiene la responsabilidad de realizar evaluaciones técnicas y aprobar formalmente todas las versiones de firmware y Software antes de su implementación en producción. También debe ejecutar análisis de compatibilidad, evaluación de impacto y validación de funcionalidad para garantizar que las actualizaciones cumplan con los estándares institucionales de calidad y seguridad.

Es fundamental que la Dirección mantenga una comunicación oportuna y clara con todo el personal técnico y administrativo responsable, proporcionando cronogramas detallados, instrucciones específicas y consideraciones especiales para cada tipo de actualización. Asimismo, debe coordinar y ejecutar directamente las actualizaciones, ya sea mediante implementación propia o en colaboración con otras instituciones y proveedores.

La Dirección de Servicios Tecnológicos debe mantener documentación completa y actualizada de todas las actualizaciones implementadas, garantizando que esta información sea accesible y esté organizada sistemáticamente para facilitar el control de cambios, auditorías de seguridad y resolución de problemas futuros.

Finalmente, es responsabilidad de la Dirección de Servicios Tecnológicos dar seguimiento a los avisos de seguridad, boletines técnicos y comunicaciones oficiales de los proveedores para identificar vulnerabilidades emergentes y tomar medidas preventivas oportunas. Adicionalmente, debe implementar y mantener un inventario actualizado y preciso de todos los dispositivos de red, incluyendo información detallada sobre firmware, Software, configuraciones y estado de soporte.

CAPÍTULO XLII
DE LA POLÍTICA DE CONCIENTIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. Propósito y Objetivo

En esta política se establecen las directrices fundamentales del Programa de Concientización en Seguridad de la Información de la SESEA. Su propósito principal es educar y sensibilizar a todo el personal sobre las prácticas seguras en el manejo de sistemas, datos y activos tecnológicos organizacionales.

El programa busca crear una cultura de seguridad integral que permita a cada colaborador identificar, prevenir y responder adecuadamente ante posibles amenazas cibernéticas. A través de la capacitación continua y la concientización, se pretende reducir significativamente el riesgo de incidentes de seguridad causados por error humano, desconocimiento o negligencia en el cumplimiento de las mejores prácticas de Ciberseguridad.

II. Alcance

Este programa de concientización aplica de manera obligatoria a todo el personal que tenga acceso directo o indirecto a la información, sistemas o infraestructura tecnológica de la SESEA, independientemente de su modalidad de contratación o tiempo de permanencia en la organización.

El alcance comprende a los empleados de base y de confianza que forman parte de la estructura organizacional permanente, así como a los prestadores de servicios profesionales que requieren acceso a recursos institucionales para el desarrollo de sus actividades. También incluye a consultores y personal externo que, por la naturaleza de sus funciones, han recibido autorización específica para acceder a sistemas o información sensible de la SESEA.

Las nuevas contrataciones y usuarios temporales quedan igualmente sujetos a estas disposiciones desde el momento de su incorporación, asegurando que toda

persona que interactúe con los activos de información de la SESEA cuente con el nivel de conocimiento necesario para proteger la integridad, confidencialidad y disponibilidad de los mismos.

III. **Descripción de la política**

El contenido que se debe brindar en la concientización debería estar enfocado principalmente en los puntos siguientes:

a) **Fundamentos de seguridad.** Los fundamentos de seguridad de la información incluyen los principios básicos de confidencialidad, integridad y disponibilidad de la información. El personal de la SESEA debe ser capaz de comprender cómo estos principios se aplican en sus actividades diarias y por qué son esenciales para la protección de los activos institucionales;

b) **Políticas y normas internas.** Las políticas y normas internas constituyen un pilar fundamental, para la protección de contraseñas, equipo y de las buenas prácticas en el uso de los activos tecnológicos de la SESEA. Es crucial que todo el personal comprenda no sólo qué está permitido, sino también las razones detrás de cada restricción o recomendación;

c) **Gestión de contraseñas.** La gestión de contraseñas requiere atención especial, desde la creación y mantenimiento de contraseñas, hasta la implementación de autenticación multifactor cuando esté disponible, y la comprensión de por qué las contraseñas débiles representan una de las principales vulnerabilidades;

d) **Ingeniería social y phishing.** Es importante que el personal de la SESEA sea capaz de identificar y responder adecuadamente ante intentos de fraude, suplantación de identidad y manipulación psicológica. Este personal debe desarrollar habilidades para reconocer señales de alerta en comunicaciones sospechosas y saber cómo proceder ante estas situaciones;

e) **Manejo de información sensible.** El manejo de información sensible abarca desde la protección de datos personales, información financiera y documentos clasificados, en estos documentos existen datos sensibles,

por ello es fundamental que el personal comprenda su responsabilidad en la custodia de información y las consecuencias de su mal manejo;

f) **Seguridad física.** La seguridad física incluye la restricción de acceso a personal no autorizado a instalaciones y equipos. Este tipo de seguridad en conjunto con la seguridad digital es un buen complemento; y,

g) **Respuesta a incidentes.** Una buena práctica es capacitar al personal que labora en la SESEA para que sea capaz de reconocer, reportar y responder apropiadamente ante anomalías o sospechas de incidentes de seguridad, para ello se deben establecer canales claros de comunicación.

Finalmente, el uso seguro de dispositivos móviles y medios extraíbles es una vulnerabilidad a los datos de la SESEA, por ello es recomendable proteger la información cuando se trabaja fuera de la oficina.

IV. **Responsabilidades**

El personal que labora en la SESEA tiene la responsabilidad de participar activamente en todas las sesiones de capacitación programadas y realizar una evaluación, con la cual se va a medir la comprensión y retención de los conceptos presentados durante la capacitación. Además de aplicar conscientemente las buenas prácticas aprendidas en su trabajo diario y reportar inmediatamente cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información institucional.

La Dirección de Servicios Tecnológicos y Plataforma Digital, deben tener un registro detallado y actualizado de participantes a las capacitaciones virtuales y físicas, fechas de realización de las sesiones, resultados obtenidos en las evaluaciones y un inventario, cursos y materiales utilizados; que incluyen infografías educativas, guías rápidas de referencia y simulaciones interactivas para experimentar situaciones reales de riesgo en entornos controlados. La capacitación se enriquecerá con casos reales y ejemplos documentados de incidentes de seguridad ocurridos en otras organizaciones similares, lo que permitirá ilustrar de manera práctica los riesgos potenciales y las consecuencias de no seguir las mejores prácticas. Este registro servirá como evidencia del cumplimiento de la política y como base para identificar áreas de mejora en el programa de capacitación.

Las capacitaciones se llevarán a cabo cada vez que se incorpore nuevo personal a la SESEA, ocurran incidentes de seguridad significativos o cuando se implementen cambios importantes en la normativa aplicable, regulaciones internas o cuando se identifiquen nuevas amenazas o vulnerabilidades que requieran atención inmediata del personal.

CAPÍTULO XLIII
DE LA POLÍTICA DE CAPACITACIÓN SOBRE INGENIERÍA SOCIAL

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. **Propósito y Objetivo**

Esta política establece la obligatoriedad de capacitar integralmente al personal de la SESEA en materia de Ciberseguridad, con el propósito de desarrollar las competencias necesarias para identificar, prevenir y reportar de manera efectiva los ataques de ingeniería social. La capacitación se enfoca particularmente en las modalidades más comunes y peligrosas que enfrentan las instituciones públicas en la actualidad, incluyendo phishing, smishing y vishing, proporcionando al personal las herramientas y conocimientos indispensables para proteger tanto la información institucional como los sistemas tecnológicos de la organización.

II. **Alcance**

Esta política de capacitación tiene un alcance integral que abarca a todo el personal que tenga interacción con los sistemas de información, correos electrónicos institucionales, dispositivos móviles corporativos o líneas telefónicas oficiales de la SESEA. El universo de aplicación incluye de manera específica a los empleados de planta y temporales que forman parte de la estructura organizacional, así como a prestadores de servicios externos y contratistas que, en virtud de sus funciones, requieren acceso a los recursos tecnológicos institucionales. Asimismo, contempla al personal externo que cuenta con autorización formal para acceder a los sistemas de información, garantizando que todas las personas con capacidad de interactuar con la infraestructura tecnológica institucional cuenten con la preparación adecuada para enfrentar las amenazas de ingeniería social.

III. **Descripción de la política**

La concientización sobre ingeniería social es muy importante, porque en muchas actividades es la manera más fácil donde se fuga la información. Por ello, es fundamental que todo el personal que labora en la SESEA, ya sea de estructura o

por honorarios, tengan en cuenta al menos las siguientes situaciones, las cuales corresponden a las principales amenazas de ingeniería social.

a) **Phishing**. El phishing se centra en el reconocimiento de correos electrónicos fraudulentos diseñados para obtener credenciales de acceso, información personal sensible o instalar Software malicioso en los sistemas institucionales. Es fundamental que el personal de la SESEA aprenda a identificar señales características como errores gramaticales, direcciones URL sospechosas, solicitudes urgentes de información y otros indicadores que revelan la naturaleza maliciosa de estas comunicaciones;

b) **Smishing**. En el smishing aborda la problemática de los mensajes de texto fraudulentos enviados a dispositivos móviles, en este escenario, los atacantes suplantan la identidad de instituciones reconocidas o servicios legítimos para engañar a los usuarios. Es importante hacer conciencia en el personal de la SESEA para que puedan reconocer enlaces peligrosos, números telefónicos sospechosos y técnicas de manipulación psicológica empleadas en estos ataques; y,

c) **Vishing**. El vishing se enfoca en las llamadas telefónicas donde los atacantes emplean técnicas de manipulación para obtener información confidencial o convencer a los usuarios de ejecutar acciones comprometedoras, frecuentemente haciéndose pasar por proveedores de servicios, personal técnico o figuras de autoridad.

IV. **Responsabilidades**

El personal que labora en la SESEA tiene la responsabilidad de participar activamente en todas las sesiones de capacitación programadas y realizar una evaluación, con la cual se va a medir la comprensión y retención de los conceptos presentados durante la capacitación. Además de aplicar conscientemente las buenas prácticas aprendidas en su trabajo diario y reportar inmediatamente cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información institucional.

La Dirección de Servicios Tecnológicos y Plataforma Digital, debe tener un registro detallado y actualizado de participantes a las capacitaciones virtuales y físicas,

fechas de realización de las sesiones, resultados obtenidos en las evaluaciones y un inventario, cursos y materiales utilizados; que incluyen infografías educativas, guías rápidas de referencia y simulaciones interactivas para experimentar situaciones reales de riesgo en entornos controlados. La capacitación se enriquecerá con casos reales y ejemplos documentados de incidentes de seguridad ocurridos en otras organizaciones similares, lo que permitirá ilustrar de manera práctica los riesgos potenciales y las consecuencias de no seguir las mejores prácticas de Ciberhigiene. Este registro servirá como evidencia del cumplimiento de la política y como base para identificar áreas de mejora en el programa de capacitación.

Las capacitaciones se llevarán a cabo cada vez que se incorpore nuevo personal a la SESEA, ocurran incidentes de seguridad significativos o cuando se implementen cambios importantes en la normativa aplicable, regulaciones internas o cuando se identifiquen nuevas amenazas o vulnerabilidades que requieran atención inmediata del personal.

V. **Normativas de Referencia**

Esta política se fundamenta en estándares internacionales reconocidos que establecen las mejores prácticas en materia de concienciación y capacitación en seguridad de la información. La norma ISO/IEC 27001:2022 en su control A.6.3 proporciona directrices para la concienciación, educación y formación en seguridad, estableciendo los principios fundamentales que guían el desarrollo de programas efectivos de capacitación.

Los CIS Controls v8 en su Control 14 abordan específicamente la capacitación en concienciación de seguridad y desarrollo de habilidades, proporcionando un marco estructurado para la implementación de programas de capacitación integral.

Las publicaciones NIST SP 800-50 y NIST SP 800-16 ofrecen metodologías probadas para la construcción de programas de concienciación y capacitación en seguridad de TI, incluyendo enfoques basados en roles que permiten personalizar la capacitación según las responsabilidades específicas de cada puesto de trabajo.

CAPÍTULO XLIV
DE LA POLÍTICA DE CAPACITACIÓN EN BUENAS PRÁCTICAS DE AUTENTICACIÓN

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. **Propósito y Objetivo**

Esta política tiene como finalidad establecer las directrices necesarias para capacitar a todo el personal de la SESEA en las mejores prácticas de autenticación. Su propósito principal es prevenir accesos no autorizados en los sistemas institucionales y garantizar la protección integral de la confidencialidad, integridad y disponibilidad de la información que se maneja en dicha Secretaría.

Con la implementación de esta política se busca crear una cultura de seguridad informática sólida, donde cada integrante del equipo comprenda la importancia de sus acciones en la protección de los activos digitales institucionales y desarrolle las competencias necesarias para actuar como primera línea de defensa contra las amenazas cibernéticas.

II. **Alcance**

Esta política abarca a todo el personal que tenga acceso a sistemas, plataformas, correos electrónicos o aplicaciones institucionales de la SESEA, sin excepción alguna. El alcance incluye al personal de base y temporales que forman parte de la plantilla laboral, así como a contratistas y personal externo que haya sido debidamente autorizado para acceder a los recursos tecnológicos.

De manera particular, se presta especial atención a aquellos usuarios que manejan sistemas o cuentan con privilegios administrativos, ya que su nivel de acceso representa un riesgo mayor para la seguridad institucional. Estos usuarios deberán cumplir con requisitos adicionales y recibir capacitación especializada acorde a sus responsabilidades específicas.

III. **Descripción de la política**

El contenido de las capacitaciones debería estar enfocado principalmente en los siguientes puntos:

Tema	Contenido sugerido
Contraseñas seguras	Requisitos mínimos de acuerdo con la Política de Uso de Contraseñas Únicas y Requisitos de Longitud (longitud, complejidad, caracteres especiales).
	Evitar contraseñas obvias, repetidas o basadas en información personal.
	No reutilizar contraseñas en múltiples sistemas, especialmente entre sistemas personales y laborales.
Gestión segura de credenciales	No compartir contraseñas con compañeros, superiores ni personal externo.
	No escribir contraseñas en papel ni guardarlas en documentos sin cifrado.
	Uso de gestores de contraseñas seguros (recomendados: Bitwarden, 1Password, KeePass).
Autenticación multifactor (MFA)	Qué es MFA y por qué es una medida de seguridad.
	Tipos de factores: algo que sabes (contraseña), algo que tienes (token, app), algo que eres (biometría).
	Sistemas institucionales que deben implementar MFA obligatoriamente.
Reconocimiento de malas prácticas	Identificar intentos de suplantación o phishing que buscan capturar credenciales.
	No ingresar contraseñas en sitios sospechosos o no verificados (verificar dominio, certificado SSL).
	Recomendaciones al usar equipos compartidos o públicos: cerrar sesión, no guardar contraseñas, limpiar historial y portapapeles.

IV. **Responsabilidades**

El personal que labora en la SESEA tiene la responsabilidad de participar activamente en todas las sesiones de capacitación programadas y realizar una evaluación, con la cual se va a medir la comprensión y retención de los conceptos presentados durante la capacitación. Además de aplicar conscientemente las buenas prácticas aprendidas en su trabajo diario y reportar inmediatamente cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información institucional.

La Dirección de Servicios Tecnológicos y Plataforma Digital, deben tener un registro detallado y actualizado de participantes a las capacitaciones virtuales y físicas, fechas de realización de las sesiones, resultados obtenidos en las evaluaciones y un inventario, cursos y materiales utilizados; que incluyen infografías educativas, guías rápidas de referencia y simulaciones interactivas para experimentar situaciones reales de riesgo en entornos controlados. La capacitación se enriquecerá con casos reales y ejemplos documentados de incidentes de seguridad ocurridos en otras organizaciones similares, lo que permitirá ilustrar de manera práctica los riesgos potenciales y las consecuencias de no seguir las mejores prácticas. Este registro servirá como evidencia del cumplimiento de la política y como base para identificar áreas de mejora en el programa de capacitación.

Las capacitaciones se llevarán a cabo cada vez que se incorpore nuevo personal a la SESEA, ocurran incidentes de seguridad significativos o cuando se implementen cambios importantes en la normativa aplicable, regulaciones internas o cuando se identifiquen nuevas amenazas o vulnerabilidades que requieran atención inmediata del personal.

V. **Normativas de Referencia**

Esta política se fundamenta en estándares internacionales reconocidos para asegurar su alineación con las mejores prácticas globales en Ciberseguridad. Se basa en la norma ISO/IEC 27001:2022, específicamente en el control A.6.3 que establece los requisitos para concienciación, educación y formación en seguridad de la información. También incorpora las directrices de CIS Controls v8, particularmente los controles 4.8 y 4.9 que abordan la implementación de autenticación multifactor y la gestión segura de credenciales. Finalmente, se alinea con las pautas establecidas en NIST SP 800-63B, que proporciona lineamientos

específicos para la autenticación de identidad digital en entornos gubernamentales y organizacionales.

CAPÍTULO XLV

DE LA POLÍTICA DE CAPACITACIÓN PARA EL MANEJO SEGURO DE DATOS CONFIDENCIALES

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. **Propósito y Objetivo**

En el presente Manual se establece el programa integral de capacitación para el manejo seguro de datos confidenciales de la SESEA, diseñado para fortalecer las competencias de todo el personal en el manejo seguro de información confidencial. El programa abarca desde la identificación correcta de datos sensibles hasta su almacenamiento, transferencia, archivo y destrucción segura, complementándose con las mejores prácticas para mantener entornos de trabajo digitales y físicos seguros.

La finalidad de esta política es garantizar que cada integrante del equipo comprenda cabalmente sus responsabilidades en la protección de la información institucional y desarrolle las habilidades necesarias para manejarla de manera segura y eficiente. Esto permite minimizar significativamente los riesgos de divulgación no autorizada, pérdida accidental o robo de información, protegiendo así la integridad institucional y el cumplimiento de nuestros objetivos anticorrupción.

II. **Alcance**

Este programa de capacitación tiene aplicación universal dentro de la SESEA, abarcando sin excepción a todo el personal de base, contratistas temporales, consultores externos, becarios y cualquier otra persona que, en el ejercicio de sus funciones, tenga acceso directo o indirecto a datos confidenciales de la SESEA. Esta cobertura integral asegura que todos los actores involucrados en el manejo de información institucional mantengan los mismos estándares de seguridad y confidencialidad.

III. **Descripción de la política**

El contenido de las capacitaciones debería estar enfocado principalmente en los puntos siguientes:

a) **Identificación de Datos Confidenciales.** El personal de la SESEA debe desarrollar las competencias necesarias para reconocer de manera precisa los diferentes tipos de datos confidenciales que maneja la SESEA en sus operaciones diarias. Así como aplicar criterios de clasificación según niveles de confidencialidad, distinguir entre información de acceso restringido, confidencial para uso interno y datos de circulación limitada. Se debe enfatizar la importancia del etiquetado y marcado adecuado de datos confidenciales tanto en formato físico como electrónico, estableciendo sistemas claros de identificación visual que permitan un manejo apropiado por parte de todo el personal;

b) **Almacenamiento Seguro de Datos Confidenciales.** El almacenamiento seguro de datos confidenciales en formato físico, así como el uso apropiado de archivadores con cerradura, bóvedas de seguridad y espacios de almacenamiento controlado son las mejores acciones para el resguardo seguro de información. En el ámbito electrónico, las mejores prácticas son el uso de carpetas en dispositivos físicos como en la nube, que estén protegidas con contraseña siguiendo la "Política de Uso de Contraseñas Únicas y Requisitos de Longitud", implementación de cifrado de datos y establecimiento de controles de acceso;

c) **Transferencia Segura de Datos Confidenciales.** Es indispensable que en las capacitaciones se establezcan claramente los métodos aprobados para transferir datos confidenciales dentro del entorno institucional de la SESEA, incluyendo el empleo de correo electrónico cifrado, sistemas de transferencia de archivos seguros y protocolos de comunicación interna.

Para las transferencias externas, se deben detallar los procedimientos autorizados que incluyen protocolos de transferencia de archivos seguros, uso de redes privadas virtuales (VPN) y canales de comunicación certificados.

Al igual que estas, se debe hacer especial énfasis en la prohibición absoluta de transferir datos confidenciales a través de canales no seguros, como correo electrónico sin cifrado o servicios de intercambio de archivos públicos. Además de las transferencias de información, es importante que todo el personal aprenda de los procedimientos para

verificar la identidad de los destinatarios antes de realizar cualquier transferencia de datos confidenciales, incluyendo métodos de autenticación y confirmación de autorización;

d) **Almacenamiento Seguro de Datos Confidenciales.** Es importante que el personal de la SESEA conozca los procedimientos para el almacenamiento adecuado de datos confidenciales, que si bien dejaron de utilizarse de manera frecuente, deben de conservarse por requisitos legales, reglamentarios u operativos. Por ello, es indispensable que se establezcan protocolos para el almacenamiento a largo plazo de datos confidenciales, incluyendo la implementación de controles de acceso, sistemas de etiquetado temporal y mecanismos de seguimiento y trazabilidad.

   Todo el personal autorizado de la SESEA debe conocer los procedimientos para recuperar datos confidenciales archivados cuando sea necesario, incluyendo procesos de autorización, registro de acceso y verificación de integridad de la información recuperada;

e) **Destrucción Segura de Datos Confidenciales.** La capacitación que se imparta al personal de la SESEA debe cubrir los métodos aprobados para la destrucción segura de datos confidenciales en formato físico, incluyendo técnicas de trituración, incineración controlada y otros métodos certificados de destrucción documental. Para el formato electrónico, se deben enseñar métodos de borrado seguro, desmagnetización de dispositivos de almacenamiento y destrucción física certificada de medios de almacenamiento.

   En dicha capacitación se debe resaltar la prohibición de desechar datos confidenciales en la basura regular o mediante métodos no seguros, y se deben detallar los requisitos obligatorios para documentar adecuadamente todos los procesos de destrucción de datos confidenciales, incluyendo registros de fecha, método utilizado y personal responsable; y,

f) **Mejores Prácticas de Pantalla Limpia y Escritorio Limpio.** Es requisito fundamental el bloqueo automático de pantallas de computadoras y otros dispositivos electrónicos cuando se dejan desatendidos, incluso por

períodos cortos. Está prohibido dejar información confidencial visible en pantallas cuando no se está utilizando activamente, y activar el cierre de sesión en aplicaciones y sistemas que contengan datos confidenciales al finalizar la jornada laboral o al alejarse del dispositivo.

En cuanto al escritorio limpio, el personal de la SESEA debe conocer el requisito obligatorio de guardar todos los documentos que contengan datos confidenciales en archivadores cerrados con llave o en áreas seguras designadas cuando no se estén utilizando activamente.

En la capacitación se deben incluir procedimientos detallados para el desecho seguro de documentos en papel que contengan datos confidenciales, pautas para borrar pizarras físicas y virtuales inmediatamente después de reuniones o presentaciones donde se haya mostrado información confidencial.

IV. **Responsabilidades**

El personal que labora en la SESEA tiene la responsabilidad de participar activamente en todas las sesiones de capacitación programadas y realizar una evaluación, con la cual se va a medir la comprensión y retención de los conceptos presentados durante la capacitación. Además de aplicar conscientemente las buenas prácticas aprendidas en su trabajo diario y reportar inmediatamente cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información institucional.

La Dirección de Servicios Tecnológicos y Plataforma Digital, deben tener un registro detallado y actualizado de participantes a las capacitaciones virtuales y físicas, fechas de realización de las sesiones, resultados obtenidos en las evaluaciones y un inventario, cursos y materiales utilizados; que incluyen infografías educativas, guías rápidas de referencia y simulaciones interactivas para experimentar situaciones reales de riesgo en entornos controlados. La capacitación se enriquecerá con casos reales y ejemplos documentados de incidentes de seguridad ocurridos en otras organizaciones similares, lo que permitirá ilustrar de manera práctica los riesgos potenciales y las consecuencias de no seguir las mejores prácticas. Este registro servirá como evidencia del cumplimiento de la política y como base para identificar áreas de mejora en el programa de capacitación.

Las capacitaciones se llevarán a cabo cada vez que se incorpore nuevo personal a la SESEA, ocurran incidentes de seguridad significativos o cuando se implementen cambios importantes en la normativa aplicable, regulaciones internas o cuando se identifiquen nuevas amenazas o vulnerabilidades que requieran atención inmediata del personal.

CAPÍTULO XLVI
DE LA POLÍTICA DE CONCIENTIZACIÓN SOBRE EXPOSICIÓN NO INTENCIONAL DE DATOS

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. Propósito y Objetivo

Esta política se enfoca en desarrollar competencias básicas para identificar, prevenir y mitigar situaciones que puedan ocasionar la exposición no intencional de datos institucionales. El objetivo principal es crear una cultura de seguridad que proteja la información sensible mediante la reducción de errores humanos y el fortalecimiento de los procedimientos de manejo de datos, garantizando así la integridad y confidencialidad de la información.

II. Alcance

Esta política tiene aplicación a todo el personal que, en el ejercicio de sus funciones, genere, gestione, manipule, transmita, almacene o tenga acceso a información institucional o confidencial, ya sea en físico o en formato digital. El alcance incluye tanto al personal de planta y temporal que forma parte de la estructura organizacional, así como a los prestadores de servicios externos que requieran acceso a sistemas institucionales. También comprende a consultores y asesores que cuenten con autorización formal para acceder a información sensible, además de todo el personal que utilicen dispositivos móviles, portátiles o cualquier equipo tecnológico proporcionado por la SESEA para el desempeño de sus actividades laborales.

III. Descripción de la política

La concientización sobre la exposición no intencional de datos es muy importante, porque en muchas actividades diarias se pueden cometer errores, o bien despreciar actividades o acciones, que, si bien no generan directamente un daño o error, pueden intervenir en más acciones y generar problemas a largo plazo. Por ello, es fundamental que todo el personal que labora en la SESEA, ya sea de estructura o por honorarios, tengan en cuenta al menos las siguientes situaciones, las cuales pueden ser el origen de fuga de información.

a) **Entrega incorrecta de información.** Es importante verificar meticulosamente la identidad del destinatario antes de enviar correos electrónicos o documentos físicos. La importancia de revisar cuidadosamente las direcciones de correo electrónico, es una tarea muy importante, en especial en casos de nombres similares o dominios parecidos que puedan generar confusión. Además, es relevante conocer el uso adecuado de los campos CC (con copia) y CCO (con copia oculta) para proteger la privacidad de los destinatarios, y evitar la exposición innecesaria de información de contacto;

b) **Revisión previa de archivos adjuntos.** La validación exhaustiva del contenido, extensión y destinatario de todos los archivos adjuntos antes de su envío, es una actividad que puede evitar la fuga de información. Es muy importante verificar que los documentos no contengan información confidencial no requerida para el propósito específico de la comunicación, esto incluye metadatos ocultos que revelen información sensible;

c) **Pérdida, extravío o robo de dispositivos.** Es necesario tomar medidas preventivas como la configuración obligatoria de bloqueo de pantalla con contraseñas seguras en los equipos de cómputo, así como la implementación de cifrado de disco completo y no dejar dispositivos sin supervisión en espacios públicos o compartidos. Protocolos claros sobre cómo mantener la custodia física de los equipos y qué hacer en situaciones de riesgo, incluyendo el uso de cables de seguridad y la selección de ubicaciones seguras para el trabajo remoto, son actividades que ayudan para no compartir información que ponga en riesgo a la SESEA.

   Ahora bien, en caso de que el equipo de cómputo asignado haya sido robado o extraviado, se debe reportar de manera inmediata a la Dirección de Servicios Tecnológicos y Plataforma Digital y Secretaría Técnica. Esto para revocar permisos, y tomar las medidas necesarias para minimizar la exposición de datos almacenados en dicho dispositivo, incluyendo el cambio de contraseñas y la notificación a contactos relevantes sobre el incidente;

d) **Publicación no autorizada de datos.** Los riesgos asociados con compartir información institucional en redes sociales, sitios web públicos o con proveedores que no cuenten con convenios de confidencialidad establecidos son un riesgo también de fuga de información. Es importante crear lineamientos sobre qué tipo de información puede ser compartida públicamente y cuál debe mantenerse estrictamente confidencial;

e) **Uso inadecuado de almacenamiento compartido.** Si bien el almacenamiento en la nube es una herramienta necesaria en las labores diarias, su uso debe estar regulado sobre las mejores prácticas. Esto porque una mala configuración en plataformas de almacenamiento en la nube como Google Drive, OneDrive, Dropbox y similares, permite accesos no autorizados a información sensible, y puede ser manipulada, incluso hasta ser eliminada, o difundida, lo cual es un riesgo potencial en la integridad de datos de la SESEA;

f) **Errores comunes al manejar documentos impresos.** Es importante establecer procedimientos para la destrucción segura de documentos confidenciales y contar con técnicas para minimizar la impresión innecesaria de información sensible, promoviendo el uso de medios digitales seguros cuando sea posible;

g) **Documentos confidenciales visibles.** Se debe implementar la política de "escritorio limpio", es decir, establecer políticas para evitar dejar documentos visibles en escritorios, salas de juntas o espacios públicos. Esto con el fin de guardar adecuadamente los documentos físicos al finalizar la jornada laboral, o al ausentarse del lugar de trabajo, y organizar el espacio de trabajo para minimizar la exposición accidental de información confidencial; y,

h) **Uso irresponsable del portapapeles digital.** Existen riesgos asociados con copiar y pegar información sensible entre diferentes documentos, correos electrónicos o aplicaciones de mensajería, por ello es fundamental contar con herramientas para limpiar regularmente el portapapeles del sistema y establecerá mejores prácticas para el manejo seguro de información temporal almacenada en memoria durante las operaciones de copiado y pegado.

IV. Responsabilidades

El personal que labora en la SESEA tiene la responsabilidad de participar activamente en todas las sesiones de capacitación programadas y realizar una evaluación, con la cual se va a medir la comprensión y retención de los conceptos presentados durante la capacitación. Además de aplicar conscientemente las buenas prácticas aprendidas en su trabajo diario y reportar inmediatamente cualquier incidente o situación sospechosa que pueda comprometer la seguridad de la información institucional.

La Dirección de Servicios Tecnológicos y Plataforma Digital, deben tener un registro detallado y actualizado de participantes a las capacitaciones virtuales y físicas, fechas de realización de las sesiones, resultados obtenidos en las evaluaciones y un inventario cursos y materiales utilizados; que incluyen infografías educativas, guías rápidas de referencia y simulaciones interactivas para experimentar situaciones reales de riesgo en entornos controlados. La capacitación se enriquecerá con casos reales y ejemplos documentados de incidentes de seguridad ocurridos en otras organizaciones similares, lo que permitirá ilustrar de manera práctica los riesgos potenciales y las consecuencias de no seguir las mejores prácticas de Ciberhigiene. Este registro servirá como evidencia del cumplimiento de la política y como base para identificar áreas de mejora en el programa de capacitación.

Las capacitaciones se llevarán a cabo cada vez que se incorpore nuevo personal a la SESEA, ocurran incidentes de seguridad significativos o cuando se implementen cambios importantes en la normativa aplicable, regulaciones internas o cuando se identifiquen nuevas amenazas o vulnerabilidades que requieran atención inmediata del personal.

V. Normativas de referencia

Esta política se fundamenta en estándares internacionales y normativas nacionales reconocidas, incluyendo el ISO/IEC 27001:2022 en su apartado A.6.3 sobre Educación en seguridad de la información, que establece los requisitos para programas de concienciación y capacitación. También se basa en los CIS Controls v8, específicamente el Control 14.4 sobre Training to Reduce Unintentional Data Exposure, que proporciona directrices para reducir la exposición no intencional de

datos. Se alinea con las recomendaciones del NIST SP 800-50 sobre IT Security Awareness and Training, que define las mejores prácticas para programas de concienciación en seguridad. Finalmente, cumple con los requisitos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México, garantizando el cumplimiento del marco legal nacional en materia de protección de datos personales.

CAPÍTULO XLVII
DE LA POLÍTICA DE IDENTIFICACIÓN Y REPORTE DE INCIDENTES DE SEGURIDAD

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. Propósito y Objetivo

La identificación temprana de incidentes de seguridad es valiosa para minimizar el impacto y preservar la continuidad operativa de la SESEA. Esta política tiene como finalidad garantizar que todo el personal de la SESEA cuente con las competencias necesarias para identificar, evaluar y reportar de manera oportuna cualquier incidente de seguridad de la información que pueda comprometer los activos digitales institucionales.

El propósito de esta política es establecer un mecanismo de respuesta rápida que permita contener posibles daños, realizar investigaciones exhaustivas sobre las causas de los incidentes y aplicar las medidas correctivas correspondientes para fortalecer la postura de seguridad organizacional.

II. Alcance

El presente documento establece lineamientos aplicables a todo el personal de la SESEA que, en el ejercicio de sus funciones, utilicen los sistemas de información institucionales o tengan acceso a datos electrónicos de la organización. Esta política abarca tanto al personal de planta como a colaboradores temporales que desempeñen actividades dentro de la SESEA, incluyendo también a contratistas externos y consultores que requieran acceso a recursos tecnológicos para el cumplimiento de sus responsabilidades. Asimismo, se extiende a usuarios que operen bajo modalidades de trabajo remoto o que utilicen dispositivos móviles para acceder a la información institucional, independientemente de su ubicación física.

III. Descripción de la política

Un incidente de seguridad se relaciona a cualquier evento que sea confirmado o bajo sospecha, o que tenga el potencial de afectar negativamente la confidencialidad, integridad o disponibilidad de los activos de información. Estos

eventos pueden manifestarse como violaciones deliberadas a las políticas de seguridad, fallas técnicas en los sistemas, errores humanos o actividades maliciosas dirigidas contra la infraestructura tecnológica. Así como la detección o sospecha de software malicioso como virus, ransomware o troyanos que puedan haber infectado los sistemas institucionales. También pueden ser accesos no autorizados a archivos, cuentas de correo electrónico o sistemas, así como cualquier fuga de información que involucre el envío accidental de documentos confidenciales a destinatarios incorrectos.

Los correos electrónicos sospechosos pueden constituir otro incidente de seguridad porque pueden ser intentos de phishing. De igual manera, la pérdida o robo de dispositivos como laptops, teléfonos celulares o unidades USB.

Los cambios no autorizados en la configuración de sistemas y los intentos de suplantación de identidad a través de llamadas telefónicas fraudulentas o mensajes de texto engañosos también constituyen incidentes de seguridad.

En caso de detectar alguno de estos incidentes, o alguno similar, debe ser reportado de inmediato. Este reporte debe ser entregado a la Dirección de Servicios Tecnológicos y Plataforma Digital, de manera física o virtual al correo electrónico plataformadigital@seseamichoacan.mx.

En casos de emergencia o cuando la naturaleza del incidente requiera intervención urgente, se puede establecer contacto telefónico directo con la Dirección a través de las extensiones 1013, 1001 o 1023. Es importante que el reporte se realice tan pronto como sea posible después de la detección del incidente, ya que la rapidez en la respuesta es fundamental para minimizar el impacto potencial.

IV. Contenido mínimo del reporte

El reporte debe incluir los datos completos de la persona que reporta, incluyendo nombre, cargo, área de adscripción y datos de contacto, esto con el fin de dar seguimiento a la situación, y de ser necesario poder solicitar más información al respecto.

Todo reporte de incidente debe incluir información específica y detallada que permita a la Dirección de Servicios Tecnológicos evaluar adecuadamente la situación y tomar las medidas correspondientes, como la fecha y hora exacta en

que se detectó el evento, y proporcionar una descripción clara y concisa de lo observado, evitando especulaciones y centrándose en los hechos verificables. Es fundamental identificar el sistema o dispositivo afectado, incluyendo información técnica relevante como números de serie, direcciones IP o nombres de usuario involucrados. Cuando sea posible y seguro hacerlo, se deben incluir capturas de pantalla que documenten visualmente el incidente, asegurándose de que estas imágenes no comprometan información adicional.

V. Responsabilidades

Esta responsabilidad es compartida y no se limita únicamente al personal técnico, sino que se extiende a todo el personal de la SESEA. Todos tienen la responsabilidad de mantenerse alerta ante posibles incidentes de seguridad y reportarlos de manera inmediata siguiendo los procedimientos establecidos.

La Dirección de Servicios Tecnológicos y Plataforma Digital, por su parte asume la responsabilidad de coordinar e implementar un programa de capacitaciones, que asegure que todo el personal cuente con los conocimientos necesarios para identificar y responder adecuadamente a los incidentes de seguridad. Esta capacitación iniciará desde el momento del ingreso del personal a la SESEA, proporcionando así una base sólida de conocimientos sobre las políticas de seguridad, procedimientos de reporte y mejores prácticas de Ciberhigiene.

La capacitación se reforzará anualmente como parte del programa institucional de concientización en seguridad, y actualizando el contenido según las nuevas amenazas y tendencias en Ciberseguridad. Adicionalmente, se implementarán campañas específicas de capacitación cuando se detecte un incremento en el nivel de riesgo o cuando se modifiquen los procedimientos establecidos, asegurando que el personal esté siempre actualizado sobre las medidas de protección vigentes.

Además de esta responsabilidad, la Dirección de Servicios Tecnológicos tiene la responsabilidad de recibir y analizar todos los reportes de incidentes, y activar los protocolos de respuesta correspondientes según la naturaleza y severidad de cada caso.

VI. Normativas de referencia

Esta política se fundamenta en estándares internacionales reconocidos para la gestión de seguridad de la información. Se alinea con los controles establecidos en

la norma ISO/IEC 27001:2022, específicamente con los apartados A.5.25 que aborda la evaluación de riesgos de seguridad de la información, A.5.26 que se refiere al tratamiento de riesgos de seguridad de la información, y A.6.3 que establece los procedimientos para el reporte de debilidades de seguridad. Asimismo, incorpora las mejores prácticas definidas en los CIS Controls v8, particularmente el Control 17.1 que establece los procesos de respuesta a incidentes y el Control 17.3 que define los procedimientos de comunicación durante incidentes. La política también se basa en las directrices establecidas en la publicación especial NIST SP 800-61r2 "Computer Security Incident Handling Guide", que proporciona un marco integral para el manejo de incidentes de seguridad informática.

CAPÍTULO XLVIII

DE LA POLÍTICA DE CAPACITACIÓN SOBRE VERIFICACIÓN Y REPORTE DE FALLAS EN ACTUALIZACIONES Y AUTOMATIZACIÓN

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. **Propósito y Objetivo**

La detección temprana de anomalías permite una respuesta rápida, efectiva, y minimiza los riesgos de seguridad, con esto se asegura la integridad y continuidad operativa de los sistemas institucionales. Por este motivo, es imprescindible que las personas servidoras públicas que laboran en la SESEA notifiquen inmediatamente al área de la Dirección de Servicios Tecnológicos cualquier irregularidad detectada en su equipo de cómputo.

Esta política tiene como propósito garantizar que todo el personal de la SESEA desarrolle las competencias necesarias para identificar de manera oportuna las fallas que puedan presentarse en los procesos de actualización de Software y en las herramientas automatizadas de seguridad y mantenimiento de su equipo de cómputo asignado.

II. **Alcance**

Esta política es de aplicación obligatoria para todo el personal que interactúe con equipos tecnológicos y sistemas institucionales, sin excepción. Comprende al personal administrativo y operativo que utilizan estaciones de trabajo fijas, equipos portátiles o cualquier Software proporcionado por la SESEA. También incluye al personal que accede a los sistemas de manera remota, así como a los usuarios que operan sistemas críticos o especializados que requieren un nivel adicional de monitoreo y cuidado.

La responsabilidad de cumplir con esta política recae en cada usuario individual, independientemente de su nivel jerárquico o función específica dentro de la SESEA.

III. **Descripción de la política**

El contenido de las capacitaciones debería estar enfocado principalmente en los puntos siguientes:

a) **Reconocimiento de software desactualizado.** El personal debe desarrollar la habilidad para identificar cuando el Software instalado en sus equipos requiere actualización. Esta competencia incluye reconocer los mensajes que emite el sistema operativo o las aplicaciones cuando detecta versiones obsoletas o cuando requieren parches de seguridad. Es fundamental que los usuarios finales puedan interpretar correctamente las alertas generadas por el antivirus o el navegador web que indican la presencia de Software sin soporte técnico o con vulnerabilidades conocidas.

   Adicionalmente, se debe fomentar la práctica de verificación visual, donde los usuarios comparen las versiones de Software instaladas en sus equipos con las versiones oficiales y recomendadas que proporciona el área de la Dirección de Servicios Tecnológicos y Plataforma Digital, asegurando así que mantengan siempre las versiones más seguras y actualizadas;

b) **Detección de fallas en procesos automatizados.** Los usuarios deben estar capacitados para verificar el correcto funcionamiento de las herramientas de seguridad automatizadas, principalmente comprobar que el antivirus se encuentre actualizado y ejecutándose sin interrupciones. Esta verificación incluye revisar que los procesos de escaneo programados se completen exitosamente y que las definiciones de virus se mantengan actualizadas.

   Es igualmente importante que el personal pueda detectar fallas en los procesos de respaldo de información, identificando a través de los reportes del sistema cuando los Backups no se han completado correctamente o presentan errores. Los usuarios también deben reconocer los mensajes de error que aparecen durante la instalación de parches o actualizaciones del sistema, especialmente aquellos que indican "actualización fallida" o procesos interrumpidos; y,

c) **Acción inmediata ante detección de fallas.** Cuando se detecte una falla o se sospeche de un riesgo de seguridad, el usuario debe suspender inmediatamente el uso del sistema afectado para evitar la propagación de problemas o la pérdida de información. Esta medida preventiva es importante para mantener la integridad de los datos y sistemas institucionales.

En este supuesto, el personal debe notificar a la Dirección de Servicios Tecnológicos de manera inmediata utilizando los canales de comunicación establecidos, que incluyen el correo electrónico oficial, el teléfono institucional o la comunicación por oficio, según corresponda a la urgencia y naturaleza de la situación. Es fundamental que los usuarios se abstengan de intentar reparar o intervenir el sistema por cuenta propia, ya que estas acciones no autorizadas pueden agravar el problema o comprometer la seguridad de la información.

IV. **Responsabilidades**

Todo el personal tiene la responsabilidad de mantener una vigilancia activa sobre el estado de sus equipos y sistemas asignados. Deben verificar regularmente la presencia de alertas, mensajes de error o comportamientos anómalos en el Software y reportar inmediatamente a la Dirección de Servicios Tecnológicos y Plataforma Digital cualquier irregularidad o anomalía detectada tanto en su equipo asignado, así como en la infraestructura tecnológica y sistemas que se administran en la SESEA. Esta responsabilidad también incluye aplicar las buenas prácticas aprendidas en las capacitaciones y participar activamente en todos los programas de formación.

La Dirección de Servicios Tecnológicos y Plataforma Digital por su parte, tiene la responsabilidad de confirmar y validar cada reporte de falla recibido, aplicando las correcciones necesarias de manera oportuna. Debe documentar cada incidente atendido, manteniendo un registro detallado de las fallas reportadas, las acciones correctivas implementadas y las medidas preventivas adoptadas para evitar la recurrencia de problemas similares.

Al igual la Dirección de Servicios Tecnológicos es la unidad responsable de buscar los cursos y material adecuados, así como difundir guías prácticas de seguridad,

crear campañas de concientización de manera periódica, y asegurar que el material educativo sea comprensible y aplicable a las diferentes unidades de la SESEA.

V. **Normativa de referencia**

Esta política se fundamenta en estándares internacionales reconocidos, incluyendo los CIS Controls v8 en sus controles 4.10 y 10.6, que establecen las mejores prácticas para la gestión segura de activos y configuraciones de software. También se alinea con la norma ISO/IEC 27001:2022 en sus anexos A.6.3 y A.8.28, que abordan la gestión de vulnerabilidades técnicas y el mantenimiento preventivo de sistemas. Adicionalmente, incorpora las mejores prácticas reconocidas internacionalmente para el mantenimiento preventivo de software, asegurando que la SESEA mantenga sus sistemas en condiciones óptimas de funcionamiento y seguridad.

VI. **Guía para reportar software desactualizado o procesos que fallaron**

El presente Manual tiene como finalidad brindar el conocimiento básico para detectar alguna falla relacionada con la actualización o procesos que fallaron en los equipos de cómputo.

VII. **Fallas comunes que debes reportar**

Los errores o fallos que surgen al actualizarse los Sistemas Operativos comúnmente están relacionados con:

- Problemas con el antivirus, dejar de funcionar o se bloquea automáticamente;
- La aparición de ventanas emergentes de publicidad tanto en el navegador, como en el escritorio del equipo de cómputo. En mucha ocasión esto surge por navegar en sitios no seguros, los cuales cargan de publicidad o infectan los equipos;
- Aplicaciones internas de la computadora, como mensajes de actualización por parte del navegador u otras aplicaciones; y,
- Mensajes de actualización del sistema operativo de Windows.

VIII. **Pasos para reportar**

La regla fundamental es no intentar resolver el problema por cuenta propia, ya que las intervenciones no autorizadas pueden agravar la situación o comprometer la seguridad del sistema. En su lugar, se debe recopilar la mayor cantidad de evidencia posible para facilitar el diagnóstico técnico.

Si es posible, tomar una captura de pantalla o fotografía del mensaje de error que aparece en la pantalla, asegurándose de que sea legible y contenga toda la información relevante. Anota el nombre exacto del Software o proceso afectado, así como una descripción detallada de las actividades que se estaba realizando antes de que se presentara la falla.

El momento para reportar es inmediatamente después de detectar cualquier anomalía. Un error aparentemente menor puede evolucionar hacia un problema de seguridad mayor si no se atiende oportunamente. La detección temprana permite implementar medidas correctivas antes de que se comprometa la integridad de los datos o la disponibilidad de los servicios. Los reportes se entregan por escrito a la Dirección de Servicios Tecnológicos, o bien pueden ser en formato digital y enviarlo a la dirección electrónica: plataformadigital@seseamichoacan.mx. Si el error parece ser grave, es recomendable informar inmediatamente por teléfono a las extensiones: 1013, 1001. 1023.

La participación activa de cada usuario en la detección y reporte de anomalías es fundamental para mantener la seguridad y disponibilidad de los sistemas institucionales. Tu vigilancia y reporte oportuno contribuyen directamente a proteger la información sensible de la SESEA y a garantizar que todos los empleados puedan realizar sus funciones sin interrupciones por problemas técnicos evitables.

CAPÍTULO XLIX

DE LA POLÍTICA DE CAPACITACIÓN SOBRE RIESGOS DE REDES INSEGURAS Y ACTIVAR SEGURIDAD EN REDES DOMÉSTICAS

CIS CONTROL #14: CONCIENTIZACIÓN DE SEGURIDAD Y CAPACITACIÓN EN HABILIDADES

I. **Propósito y objetivo**

Las redes inalámbricas públicas en su mayoría son puntos de acceso inseguros, esto dada la cantidad de dispositivos que se pueden conectar, además que, por su naturaleza, son vulnerables a ataques cibernéticos. Estos mismos ataques pueden ocurrir en redes domésticas mal configuradas o aquellas que están configuradas con parámetros por defecto. Dado este precedente, con esta política se establece la obligación de que el personal de la SESEA esté capacitado para reconocer y manejar dichos riesgos asociados con las conexiones a redes inseguras, particularmente las redes Wi-Fi públicas. Y con esto garantizar que comprendan las medidas necesarias para proteger tanto su red doméstica, así como la información institucional que pueda viajar en la red.

Con la implementación de esta política se busca crear una cultura de seguridad digital que permita al personal de la SESEA identificar amenazas potenciales y aplicar las mejores prácticas de Ciberseguridad, para fortalecer la protección integral de los activos de información de la SESEA.

II. **Alcance**

Esta política está dirigida a todo el personal de la SESEA que tenga acceso a datos institucionales, sistemas informáticos o infraestructura de la organización, para que implementen medidas de seguridad al momento de utilizar redes inalámbricas públicas.

III. **Descripción de la política**

El contenido de las capacitaciones debería estar enfocado principalmente en los puntos siguientes:

a) **Riesgos de redes públicas o inseguras.** Las redes públicas como aquellas disponibles en cafés, aeropuertos, centros comerciales y otros espacios públicos conllevan errores inherentes. Esto se debe porque, dichas redes son altamente vulnerables a ataques de tipo "man-in-the-middle", donde los atacantes pueden interceptar y manipular las comunicaciones entre el dispositivo del usuario y el servidor de destino. Por tal motivo, la transmisión de información sensible como contraseñas, correos electrónicos o documentos confidenciales a través de estas redes puede comprometer gravemente la seguridad de la información institucional;

b) **Buenas prácticas de conexión.** La capacitación se debe enfocar en la importancia de nunca acceder a sistemas institucionales desde redes públicas, sin contar con una VPN activa y debidamente configurada, además protegida por protocolos WPA2 o WPA3. También debe resaltar la importancia de no compartir conexiones móviles con dispositivos no autorizados, y cómo esta acción puede crear vulnerabilidades de seguridad, y comprometer la integridad de la información institucional; y,

c) **Seguridad en redes domésticas.** La capacitación también debe enfocarse en los pasos necesarios para asegurar las redes domésticas, mediante la cual, el personal de la SESEA puede acceder de manera remota a un solo equipo de cómputo de la SESEA. Este acceso debe ser concedido únicamente en caso de urgencia y con la previa autorización por escrito por parte de la Dirección de Servicios Tecnológicos y Plataforma Digital, así como por la Secretaría Técnica.

IV. **Responsabilidades**

El personal de la SESEA en general tiene la responsabilidad de aplicar las buenas prácticas aprendidas en las capacitaciones y participar activamente en todos los programas de formación. Así mismo deben reportar inmediatamente cualquier acceso sospechoso o situaciones donde haya utilizado redes no seguras con activos tecnológicos de la SESEA. Esto con el fin de evaluar su impacto a la seguridad y posibles incidentes.

Por su parte, la Dirección de Servicios Tecnológicos y Plataforma Digital será la responsable de buscar los cursos y material adecuados, así como difundir guías

prácticas de seguridad, crear campañas de concientización de manera periódica, y asegurar que el material educativo sea comprensible y aplicable a las diferentes unidades de la SESEA.

V. **Modalidad y frecuencia de capacitación**

La capacitación se impartirá durante los primeros días del personal nuevo, para asegurar que, desde el primer día de labores se comprendan los riesgos y medidas de protección necesarias. Posteriormente, la Dirección de Servicios Tecnológicos debe programar al menos una capacitación al año para reforzar conocimientos y actualizar al personal sobre nuevas amenazas y mejores prácticas. Además, la Dirección de Servicios Tecnológicos debe programar capacitaciones cuando se identifiquen nuevas vulnerabilidades que requieran atención inmediata del personal.

VI. **Normativas de referencia**

Esta política se fundamenta en estándares internacionales reconocidos, incluyendo los CIS Controls v8 específicamente los controles 12.6 y 14.6 relacionados con la gestión de activos y protección de datos. También se alinea con los requisitos de ISO/IEC 27001 en sus apartados A.6.3 y A.5.10 que abordan la responsabilidad de los activos y la gestión de la información. Adicionalmente, se consideran las mejores prácticas del NIST Cybersecurity Framework, particularmente en las funciones de Protección (PR.AC y PR.IP) que se relacionan con el control de acceso y la protección de la información y los procesos

VII. **Guía para asegurar una Red Wi-Fi Doméstica**

El presente Manual tiene como finalidad brindar el conocimiento básico para configurar una red inalámbrica doméstica segura.

a) **Cambia la contraseña predeterminada del módem/router.** La primera línea de defensa de una red doméstica es cambiar la contraseña predeterminada que viene configurada de fábrica. Nunca se debe utilizar contraseñas similares a "admin", "12345678" o el nombre del fabricante, ya que estas son ampliamente conocidas por los atacantes. Por ello es indispensable crear una contraseña robusta que combine letras mayúsculas y minúsculas, números y símbolos especiales, siguiendo siempre la "Política de Uso de Contraseñas Únicas y Requisitos de

Longitud" de la SESEA. También es recomendable cambiar el nombre de la red (SSID) porque los nombres por defecto revelan información sobre el fabricante o modelo del router;

b) **Usa cifrado WPA2 o WPA3.** El cifrado WPA3 es la opción más segura disponible actualmente, pero si el router no soporta dicho protocolo, WPA2 es una alternativa segura y ampliamente compatible con dispositivos más antiguos;

c) **Separa tu red doméstica de invitados.** Esta práctica de segmentación de red asegura que la red principal, donde se conectan tus dispositivos de trabajo, no se vea comprometida por dispositivos ajenos que podrían estar infectados o mal configurados. Por este motivo, es imprescindible que la red de invitados tenga una contraseña diferente a la red principal y, que tenga restricciones de acceso que limiten la conectividad entre dispositivos conectados a ella;

d) **Actualiza el firmware del router.** Los fabricantes publican frecuentemente parches de seguridad que corrigen vulnerabilidades conocidas, por lo que mantener el firmware actualizado es importante para la seguridad de la red. Algunos routers modernos incluyen la opción de actualización automática, esta opción es recomendable activar, porque sí, siempre se van a descargar las últimas correcciones de seguridad, sin necesidad de intervención manual;

e) **Desactiva funciones innecesarias.** Revisar y desactivar cualquier función que no se utiliza es una buena práctica, porque en muchas ocasiones, estas funciones pueden crear puntos de entrada para atacantes si no están debidamente configuradas; y,

f) **Usa VPN.** Para acceder a los sistemas institucionales desde alguna red doméstica, es recomendable usar una VPN (Virtual Private Network, Red Virtual Privada). Esta conexión protege los datos incluso si una doméstica tiene vulnerabilidades no detectadas.

CAPÍTULO L
DE LA POLÍTICA PARA LA GESTIÓN DEL INVENTARIO DE PROVEEDORES DE SERVICIOS

CIS CONTROL #15: GESTIÓN DE PROVEEDORES DE SERVICIOS.

I. Propósito y Objetivo

Esta política tiene como propósito establecer la obligación de mantener un inventario actualizado y completo de todos los proveedores de servicios que ofrecen productos y servicios a la SESEA. El inventario debe incluir una clasificación de cada proveedor según su nivel de riesgo para la organización, así como la designación de un responsable interno para cada relación comercial. Con esta medida se busca gestionar de manera efectiva los riesgos asociados a los servicios contratados con terceros, para garantizar el cumplimiento de los controles de seguridad establecidos y asegurando la continuidad operativa de la SESEA.

II. Alcance

Esta política aplica a todos los proveedores que mantengan una relación contractual o de servicios con la SESEA. Se incluyen específicamente aquellos que presten servicios tecnológicos, operativos, administrativos, de mantenimiento o consultoría, independientemente de la duración o modalidad del contrato. Asimismo, abarca a todos los terceros que requieran acceso a datos institucionales, sistemas informáticos o infraestructura de la organización, ya sea que este acceso se realice de forma presencial en las instalaciones o de manera remota a través de conexiones digitales. Así como a las unidades responsables en la gestión y trato con dichos proveedores, como la Dirección de Servicios Tecnológicos, la Delegación Administrativa y la Secretaría Técnica.

III. Descripción de la política

El inventario de proveedores debe estructurarse como un documento comprehensivo que contenga campos específicos para garantizar un control efectivo. Cada registro debe incluir el nombre del proveedor, así como la razón social con el nombre comercial bajo el cual opera. Además, es fundamental describir

detalladamente el tipo de servicio proporcionado, categorizándolo según su naturaleza (hosting, soporte técnico, mantenimiento, consultoría, entre otros).

En el inventario de proveedores debe especificar claramente si el proveedor tiene acceso a datos sensibles y, en caso afirmativo, detallar qué tipo de información maneja. Cada proveedor debe tener asignado un responsable interno específico, quien será la persona o área encargada de mantener la relación y realizar el seguimiento correspondiente. En la clasificación de riesgo debe asignarse utilizando los criterios establecidos en el documento complementario, categorizando cada proveedor como Alto, Medio o Bajo según sea el tipo de riesgo asignado por la Dirección de Servicios Tecnológicos y la Delegación Administrativa .

Finalmente, se debe registrar la fecha de contratación inicial del contrato vigente y la fecha de la última revisión del estatus del proveedor, garantizando la trazabilidad temporal de la relación comercial.

El inventario se puede almacenar de manera digital o física utilizando como referencia la estructura de la tabla siguiente.

Campo	Descripción
Nombre del proveedor	Razón social o nombre comercial
Servicio proporcionado	Tipo de servicio (hosting, soporte, mantenimiento, entre otros.)
Clasificación de riesgo	Alto / Medio / Bajo (ver criterios en el documento 2)
Datos sensibles tratados	¿Sí/No? ¿Qué tipo? (si aplica)
Responsable interno asignado	Persona o área responsable de la relación y seguimiento
Fecha de contratación	Fecha inicial del contrato vigente
Fecha de revisión	Última revisión del estatus del proveedor

IV. **Actualización y revisión del inventario**

El inventario debe someterse a revisión al menos una vez al año, dicho proceso debe ser documentado y respaldado adecuadamente. Adicionalmente, se debe actualizar de manera inmediata cuando se incorpore un nuevo proveedor a la cartera de servicios de la SESEA. También es necesario actualizar el registro cuando se modifique el alcance del servicio proporcionado por un proveedor existente, ya que esto puede implicar cambios en su clasificación de riesgo.

La detección de cualquier incidente relacionado con un proveedor constituye un motivo obligatorio para la actualización del inventario, incluyendo la documentación del evento y las medidas correctivas implementadas. Finalmente, cuando concluya la relación contractual con un tercero, debe registrarse esta finalización y documentar el proceso de desvinculación para mantener la integridad del inventario.

V. **Responsabilidades**

La Delegación Administrativa y Dirección de Servicios Tecnológicos y Plataforma Digital tienen la responsabilidad principal de mantener actualizado el inventario oficial de proveedores, asegurando que toda la información contenida sea precisa y esté al día. Esta función incluye la coordinación con las diferentes áreas de la organización para recopilar y validar la información necesaria.

Por su parte, la Delegación Administrativa debe asignar un responsable para supervisar de manera continua el cumplimiento del contrato, monitoreando tanto los aspectos de seguridad como el rendimiento del proveedor. Esta supervisión incluye la evaluación regular de la calidad del servicio y la identificación temprana de posibles riesgos o incumplimientos.

Y la Dirección de Servicios Tecnológicos y Plataforma Digital debe asignar un responsable para clasificar el riesgo y las implicaciones de Ciberseguridad asociadas por cada proveedor, así como proporcionar los criterios técnicos para la evaluación de riesgos y asesorar en la implementación de medidas de seguridad apropiadas.

VI. **Normativas de referencia**

Esta política se fundamenta en los estándares internacionales de seguridad y mejores prácticas reconocidas en el ámbito de la gestión de terceros. Se alinea específicamente con los CIS Controls v8, particularmente los controles 15.1 y 15.2 que abordan la gestión de proveedores de servicios. También cumple con los lineamientos establecidos en ISO/IEC 27001:2022, específicamente los controles A.5.19, A.5.20 y A.5.21 relacionados con la gestión de proveedores.

Adicionalmente, incorpora las buenas prácticas de gestión de terceros recomendadas por el Instituto Nacional de Estándares y Tecnología (NIST), particularmente las establecidas en NIST 800-161 para la gestión de riesgos de la cadena de suministro y NIST 800-53 SR para controles de seguridad relacionados con proveedores.

VII. **Criterios de clasificación de riesgos con proveedores**

a) Propósito y Objetivo

Este documento tiene como finalidad definir los criterios y metodologías mediante los cuales se asigna una clasificación de riesgo a los proveedores de servicios de la organización. La clasificación utiliza una escala de tres niveles (Alto, Medio y Bajo) basada en el análisis del impacto potencial que cada proveedor, tomando en consideración la confidencialidad, integridad y disponibilidad de la información que requieren para proporcionar un servicio a la SESEA.

b) Niveles de clasificación

1. **Alto Riesgo**. Los proveedores clasificados como Alto Riesgo son aquellos que representan un impacto significativo para la seguridad y operación de la SESEA. Esta categoría incluye proveedores que acceden, procesan o almacenan datos sensibles tales como información personal, financiera o confidencial de la SESEA. También abarca aquellos que tienen acceso a sistemas, incluyendo plataformas gubernamentales, bases de datos centrales y servidores principales de la SESEA. También se consideran de Alto

Riesgo los proveedores que brindan soporte remoto o poseen privilegios administrativos sobre activos clave de la infraestructura tecnológica. Asimismo, aquellos cuyo fallo o compromiso puede afectar significativamente la operación de la SESEA o su reputación pública;

2. **Riesgo Medio**. Esta categoría agrupa a proveedores que acceden a sistemas operativos no críticos o manejan información que no se considera sensible para la organización. Incluye personal de soporte técnico que no posee privilegios elevados en los sistemas, así como proveedores que tienen acceso físico limitado a las instalaciones de la organización sin comprometer áreas críticas; y,

3. **Riesgo Bajo**. Los proveedores clasificados como Riesgo Bajo son aquellos que no acceden a datos institucionales ni a sistemas informáticos de la organización. Proporcionan servicios generales que no tienen implicaciones directas de seguridad y su fallo no afecta la continuidad de operaciones de la SESEA de manera significativa. Esta categoría incluye servicios como limpieza, suministro de papelería, servicios de cafetería y transporte de personal.

c) Procedimiento de evaluación

La clasificación de riesgo de cada nuevo proveedor debe realizarse mediante un proceso colaborativo entre la Delegación Administrativa y la Dirección de Servicios Tecnológicos y Plataforma Digital, siempre y cuando dicho proveedor esté relacionado con los activos informáticos de la SESEA. Esta evaluación debe considerar no solo el tipo de servicio proporcionado, sino también el nivel de acceso requerido y el impacto potencial en la organización.

Todas las evaluaciones deben documentarse adecuadamente en el inventario de proveedores y conservarse como respaldo para futuras revisiones. Esta documentación debe incluir la justificación de la clasificación asignada y los criterios específicos considerados en la evaluación.

VIII. **Revisión de riesgo y proveedor**

El análisis de clasificación debe someterse al menos a una revisión anual para garantizar que la categorización siga siendo apropiada. Esta revisión debe considerar cambios en el entorno de riesgo, modificaciones en los servicios proporcionados y la experiencia operativa con el proveedor.

La revisión debe realizarse de manera extraordinaria cuando se presente un incidente de seguridad o incumplimiento contractual que involucre al proveedor. También debe ejecutarse cuando el proveedor solicite mayor acceso a sistemas o información, o cuando se modifiquen las condiciones contractuales. Finalmente, toda renovación o extensión de contrato debe incluir una revisión de la clasificación de riesgo para asegurar que sigue siendo apropiada bajo las nuevas condiciones.

CAPÍTULO LI
DE LA POLÍTICA DE MANEJO DE INCIDENTES CIBERNÉTICOS

CIS CONTROL #17: GESTIÓN DE RESPUESTA A INCIDENTES.

I. Propósito y Objetivo

Esta política se establece para la gestión de incidentes de Ciberseguridad en la SESEA, designando formalmente a la Dirección de Servicios Tecnológicos y Plataforma Digital como la principal unidad responsable de liderar la gestión de dichos incidentes.

El propósito de esta política es garantizar una respuesta oportuna, eficaz y coordinada ante cualquier tipo de incidente que pueda comprometer la seguridad de la información, los sistemas tecnológicos que integran la Plataforma Digital Estatal o las operaciones institucionales. Esto con el fin de minimizar el impacto negativo sobre las operaciones críticas, proteger la reputación institucional, y facilitar una recuperación eficiente de las operaciones normales en el menor tiempo posible.

II. Alcance

Esta política se aplica de manera integral a todos los incidentes que afecten o puedan potencialmente afectar la seguridad, operatividad y continuidad de los servicios de la SESEA. El alcance comprende incidentes de seguridad cibernética tales como violaciones de seguridad, accesos no autorizados a sistemas o información, ataques de malware, ransomware y cualquier forma de compromiso de datos sensibles.

También incluye interrupciones de servicios críticos causadas por fallos de sistemas, cortes de energía eléctrica, problemas de conectividad o fallas en la infraestructura tecnológica.

Los incidentes operativos derivados de errores en procesos críticos, fallos de equipos esenciales, problemas en la cadena de suministro tecnológico y cualquier situación que afecte los procedimientos establecidos están igualmente cubiertos.

III. **Responsabilidades**

La efectividad de esta política se basa en las responsabilidades de los principales responsables de la SESEA que se encuentran al resguardo de la información y activos informáticos. Entre ellos se destacan:

a) **La Dirección de Servicios Tecnológicos y Plataforma Digital.** La Dirección de Servicios Tecnológicos y Plataforma Digital asume la responsabilidad principal y exclusiva del manejo integral de incidentes de Ciberseguridad en la SESEA. Esta designación implica el liderazgo en todos los aspectos relacionados con la prevención, detección, respuesta y recuperación ante incidentes de cualquier naturaleza que afecten la SESEA.

   La función principal de la Dirección de Servicios Tecnológicos es crear, implementar y mantener actualizado un Plan de Respuesta a Incidentes (PRI), con el cual se reflejen las mejores prácticas tecnológicas, protocolos claros de actuación y roles definidos para cada situación. Esto con el fin de dirigir todas las actividades de respuesta a incidentes, así como para la prevención de ciberataques.

   En la Dirección de Servicios Tecnológicos se debe designar una persona que sea responsable de evaluar de manera técnica y objetiva la gravedad y el impacto real y potencial de cada incidente, utilizando criterios predefinidos que permitan una clasificación adecuada y una respuesta proporcional. Esta evaluación incluirá el análisis de riesgos, la identificación de activos afectados y la proyección de posibles consecuencias. Además, gestionará de manera para limitar el alcance del incidente, la resolución técnica del problema identificado y la recuperación completa de los servicios afectados, coordinando los recursos humanos, y técnicos. De esto, también documentará exhaustivamente todos los aspectos del incidente, incluyendo cronología detallada, acciones tomadas, recursos utilizados, hallazgos técnicos y lecciones aprendidas, generando reportes que sirvan para mejorar continuamente los procesos de respuesta.

Se designará al menos una persona de la Dirección de Servicios Tecnológicos y Plataforma Digital para supervisar y coordinar de manera efectiva el trabajo con proveedores externos durante la gestión de incidentes. Esta persona actuará como enlace principal y único punto de contacto entre la SESEA y cualquier proveedor externo involucrado en la respuesta a incidentes, evitando confusiones y asegurando una comunicación fluida y coordinada. Su responsabilidad incluye asegurar que todas las actividades realizadas por proveedores externos se alineen perfectamente con el Plan de Respuesta a Incidentes (PRI) y se cumplan con los estándares y procedimientos establecidos en esta política. Proporcionará a los proveedores externos toda la información necesaria, y apoyo logístico para ejecutar eficazmente sus funciones, manteniendo siempre el equilibrio entre la colaboración efectiva y la protección de la información sensible. Monitoreará continuamente el progreso y desempeño de los proveedores externos, garantizando que se cumplan los plazos establecidos, los objetivos de calidad y los estándares de seguridad requeridos. Revisará y aprobará todos los informes, recomendaciones y entregables producidos por los proveedores externos, asegurando que estos documentos cumplan con los estándares institucionales y proporcionen valor agregado a la gestión del incidente. Facilitará la comunicación bidireccional entre los proveedores externos y el personal interno de la SESEA, organizando reuniones de coordinación, reportes de estatus y sesiones de trabajo conjunto cuando sea necesario.

El personal de la Dirección de Servicios Tecnológicos y Plataforma Digital debe recibir capacitación especializada y continua en manejo de incidentes. Esta capacitación incluirá un conocimiento profundo del Plan de Respuesta a Incidentes (PRI) de la SESEA, asegurando que cada integrante del equipo comprenda su rol específico, las responsabilidades asignadas y los procedimientos a seguir en diferentes escenarios. La formación abarcará procedimientos detallados de manejo de incidentes, incluyendo técnicas de identificación temprana, métodos de contención, estrategias de comunicación, procesos de documentación y protocolos de recuperación. Se enfatizará el desarrollo de habilidades prácticas a través de simulacros y ejercicios que permitan al personal experimentar situaciones reales de manera controlada; y,

b) **La Secretaría Técnica.** La Secretaría Técnica es la responsable de proporcionar los recursos tecnológicos y humanos que sean necesarios en la Dirección de Servicios Tecnológicos para gestionar el manejo de incidencias cibernéticas. Además, es el contacto principal para informar a todas las personas servidoras públicas que laboran en la SESEA, acerca de los incidentes ocurridos, tanto a nivel interno con las diferentes áreas, así como con las autoridades competentes, medios de comunicación cuando sea necesario, y otras instituciones relevantes. Esta función incluye la preparación de comunicados oficiales y la coordinación de estrategias de comunicación de crisis.

Finalmente, es responsabilidad de las personas servidoras públicas que laboren en la SESEA informar a la Dirección de Servicios Tecnológicos y la Secretaría Técnica, cuando detecten actividad inusual en las instalaciones tecnológicas de la SESEA, así como actividad inusual en los activos informáticos, esto sin limitarse en los equipos de cómputo y sistemas que integran la Plataforma Digital Estatal.

CAPÍTULO LII

DE LA POLÍTICA DE GESTIÓN Y ACTUALIZACIÓN DE CONTACTOS QUE DAN RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA

CIS CONTROL #17: GESTIÓN DE RESPUESTA A INCIDENTES.

I. **Propósito y Objetivo**

La correcta gestión de contactos permite dar respuesta eficiente ante eventos de Ciberseguridad, porque con la referencia correcta se elimina la incertidumbre sobre a quién contactar en situaciones críticas, con esto, a su vez, se minimiza el impacto operacional.

Esta política tiene como finalidad establecer y mantener actualizada una agenda de contactos internos y externos que, deben ser informados cuando ocurran incidentes de seguridad informática. El propósito de esta política, es garantizar una comunicación efectiva, oportuna y conforme a los protocolos legales y contractuales establecidos por la SESEA.

II. **Alcance**

Esta política aplica tanto al personal interno, como a los proveedores de tecnologías de información y Ciberseguridad que mantengan relaciones con la SESEA. Asimismo, abarca las relaciones con autoridades legales y reguladoras, competentes, proveedores, y socios estratégicos o interinstitucionales que requieran ser notificados según la naturaleza del incidente.

III. **Descripción de la política**

La SESEA debe crear y/o mantener una agenda oficial y actualizada de las personas relacionadas, tanto en la parte técnica, como normativa, entre otras, respecto a temas de Ciberseguridad. Esta agenda debe contener al menos el nombre completo de la entidad o persona, especificando si se trata de personal interno, proveedores, autoridades reguladoras, u otros tipos de contactos relevantes. Cada contacto debe tener claramente definido su rol específico ante incidentes, identificando si su función es de naturaleza técnica, legal,

comunicacional u operativa. La información de contacto debe incluir números telefónicos directos o celulares, preferiblemente disponibles las 24 horas del día cuando sea aplicable, así como correos electrónicos oficiales y medios alternativos de contacto como SMS, WhatsApp, Telegram, Teams o sistemas de tickets. Dicha información deberá recabarse y utilizarse con apego a la normatividad en materia de transparencia y protección de datos personales.

La información por cada contacto puede ser almacenada en digital y/o en físico, usando tarjetas como se muestra en la siguiente tabla.

Campo	Descripción
Nombre de la entidad o persona	Nombre completo o razón social
Tipo de contacto	Interno, proveedor, autoridad, entre otros
Rol ante incidentes	Técnico, legal, comunicación, entre otros
Teléfono directo o celular	Disponible 24/7 si aplica
Correo electrónico oficial	
Medio alternativo de contacto	(Ej. WhatsApp, Telegram, Teams, sistema de tickets)
Fecha de última verificación	Se debe actualizar al menos 1 vez por año

Es fundamental registrar la fecha de última verificación para cada contacto, estableciendo como requisito mínimo una actualización anual de toda la información.

La agenda completa de contactos debe someterse a un proceso de verificación, y actualización al menos una vez por año. Este proceso debe incluir la confirmación directa con cada contacto registrado para validar que la información sigue siendo correcta y actualizada.

Además de la revisión anual programada, la agenda debe actualizarse de manera inmediata cuando ocurran cambios significativos en el personal clave de la organización, nuevas contrataciones o terminación de relaciones contractuales con proveedores, y cambios regulatorios que afecten los contactos que deben ser notificados según la legislación vigente.

IV. **Responsabilidades**

La **Dirección de Servicios Tecnológicos,** tiene la responsabilidad principal de mantener la lista actualizada y compartirla oportunamente con las personas servidoras públicas de la SESEA. Así mismo, la Dirección de Servicios Tecnológicos debe asegurar que todos los cambios en la agenda sean documentados y comunicados a las personas servidoras públicas de la SESEA en general.

Por su parte, la **Dirección de Normatividad y Asuntos Jurídicos y/o Delegación Administrativa,** son las responsables de validar los contactos externos, especialmente aquellos relacionados con las autoridades competentes, además deben verificar que estos contactos cumplan con los requisitos legales y contractuales aplicables.

Finalmente, la Secretaria Técnica debe aprobar los criterios de inclusión y exclusión de contactos en la lista, asegurando que se mantenga un equilibrio entre la completitud de la información y la seguridad operacional.

V. **Seguridad de la información**

La lista de contactos debe almacenarse en un lugar seguro, pero accesible para el personal de la SESEA en general, utilizando preferiblemente carpetas protegidas en institucional o servicios de almacenamiento en la nube con las debidas medidas de seguridad implementadas, y en apego a la normatividad aplicable en materia de acceso a la información y protección de datos personales.

El acceso de modificación a esta lista debe estar restringido, y se debe implementar un sistema de control de versiones, con el cual se permita rastrear los cambios realizados para mantener un historial de modificaciones para fines de auditoría.

VI. **Normativas de referencia**

Esta política se basa en las mejores prácticas internacionales establecidas por los CIS Controls v8, específicamente el Control 17.1 relacionado con la gestión de incidentes. También se alinea con los estándares ISO/IEC 27035 para la gestión de incidentes de seguridad de la información y sigue las directrices del NIST SP 800-61 Computer Security Incident Handling Guide.

VII. **Guía de notificación de incidentes**

La guía de notificación es un documento donde se establecen los procedimientos para determinar ¿Cuándo?, ¿A quién? y valorar qué tan grave es la incidencia para ser informada. Al igual en dicha guía se proporcionan los criterios para la toma de decisiones durante situaciones críticas.

VIII. **Clasificación de incidentes y notificación**

La Dirección de Servicios Tecnológicos ha detectado cuatro posibles incidencias, las cuales, dependiendo de su impacto, han sido clasificadas de la siguiente manera para su notificación:

a) **Filtración de datos personales o sensibles.** Cuando existen datos ajenos a los que usualmente son manejados por la SESEA en las diferentes áreas, o bien, aparecen usuarios que no pertenecen a dicha institución debe ser notificado inmediatamente a la Dirección de Servicios Tecnológicos, la Dirección de Normatividad y Asuntos Jurídicos, la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y la Secretaría Técnica. El tiempo máximo para dar respuesta de los posibles daños encontrados, es de 24 horas desde la detección del incidente;

b) **Ciberataque o ransomware grave.** En caso de ciberataques o infecciones por virus, la notificación también debe ser inmediata a la Dirección de Servicios Tecnológicos. El tiempo máximo para dar respuesta de los posibles daños encontrados, es de 24 horas desde la detección del incidente;

c) **Falla técnica con afectación a sistemas.** Cuando se presenten fallas en los equipos de cómputo, o dispositivos, así como fallas en los sistemas que integra la Plataforma Digital Estatal, la página oficial, así como las demás herramientas de Software que son creadas en la SESEA, y que

su inactividad afecta el funcionamiento de dicha institución. Estas incidencias deben ser informadas a más tardar una hora después a la Dirección de Servicios Tecnológicos, desde que fue detectado el incidente; y,

d) **Incidente menor sin impacto.** Estos incidentes están relacionados a intentos fallidos de acceso no autorizado, estos incidentes deben reportarse a la Dirección de Servicios Tecnológicos a más tardar 24 horas desde que fue detectado. Aunque este incidente no corresponde a un error potencial, es importante mantener el registro para análisis de tendencias.

IX. **Contenido del reporte**

Todo reporte de incidente debe contener información precisa y completa que facilite la evaluación y respuesta apropiada. Este debe incluir la fecha y hora exacta en que se detectó el incidente, el tipo específico de incidente y una descripción detallada de los sistemas afectados.

Es fundamental incluir todos los indicadores técnicos conocidos como direcciones IP sospechosas, nombres de archivos maliciosos, URLs relacionadas, o cualquier otro elemento que pueda ayudar en la investigación. El reporte debe detallar las acciones que se han tomado hasta el momento de la notificación y debe identificar claramente el nombre y datos de contacto del responsable que está reportando el incidente.

X. **Procedimiento para notificar**

La notificación principal debe realizarse a través del correo oficial **plataformadigital@seseamichoacan.mx**, asegurando que el mensaje incluya toda la información requerida en el formato establecido. Para incidentes con impacto inmediato, debe utilizarse adicionalmente el canal de emergencia disponible a través de WhatsApp o llamada telefónica directa.

Cuando el incidente afecte operaciones críticas de la SESEA, es obligatorio realizar una llamada directa a los responsables designados para garantizar la recepción inmediata del reporte y la activación de los protocolos de respuesta correspondientes.

XI. **Contactos rápidos**

Para facilitar la comunicación, se proporciona la lista de contactos siguiente:

Ente de gobierno	Unidad	Medio de contacto	Horario
SESEA	Dirección de Servicios Tecnológicos y Plataforma Digital	plataformadigital@seseamichoacan.mx	8:00–20:00
SESEA	Departamento de Servicios Tecnológicos y Plataforma Digital	plataformadigital@seseamichoacan.mx	8:00–20:00
SESEA	Dirección de Normatividad y Asuntos Jurídico	juridico@seseamichoacan.mx	Horario laboral
Policía Cibernética	Unidad Cibernética Estatal	800 890 8106	24/7
Policía Cibernética	Subdirección de la Policía Cibernética de la Secretaría de Seguridad Pública	(443) 322 8100, extensión 10211	24/7

ANEXOS

Anexo A – Formato de Solicitud para Autorización de Software / Hardware Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Michoacán
Dirección de Servicios Tecnológicos y Plataforma Digital

1. Datos del Área Solicitante
- Área solicitante: _____
- Nombre del responsable del área: _____
- Correo institucional: _____
- Fecha de solicitud: _____ / _____ / _____

---

2. Datos del Software / Hardware a Solicitar
- Nombre del software / Hardware: _____
- Versión específica (si aplica): _____
- Proveedor / Sitio de descarga oficial: _____
- Tipo de software: ☐ Comercial ☐ Gratuito ☐ De código abierto
- Licencia requerida: ☐ Sí ☐ No
- Duración / Vigencia de la licencia (si aplica): _____
- Funcionalidad / Justificación de uso:
  (Describa el propósito del software y cómo contribuye a las funciones del área)

---

3. Evaluación Técnica y de Seguridad
(A llenar por la Dirección de Servicios Tecnológicos y Plataforma Digital)
- ¿Cumple con los lineamientos de seguridad? ☐ Sí ☐ No
- ¿Es compatible con la infraestructura actual? ☐ Sí ☐ No
- ¿Requiere configuraciones especiales o acceso privilegiado? ☐ Sí ☐ No
- Observaciones técnicas:

---

4. Autorizaciones

Cargo	Nombre y Firma	Fecha
Secretaría Técnica	_____	___ / ___ / ____
Delegación Administrativa	_____	___ / ___ / ____
Dirección de Servicios Tecnológicos y Plataforma Digital	_____	___ / ___ / ____

---

5. Resolución Final
- ☐ Autorizado

- ☐ No Autorizado
- Motivo / Condiciones (en caso de autorización condicionada o rechazo):

Anexo B – Bitácora de Software

Anexo C – Matriz de Clasificación de Datos

Bitácora de Software

Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital

Número de Registro / Ticket	Nombre del Software	Versión	Proveedor / Fabricante	Nombre del Usuario Responsable	Área o Departamento	Ubicación del Equipo	Sistema Operativo	¿Se eliminará el software?	¿Se solicita excepción?	Motivo (Eliminación o Excepción)	Controles de Mitigación Aplicados	Justificación de la Eliminación o Excepción	Método de Eliminación	Fecha y Hora de Eliminación	Nuevo Software Instalado / Alternativa	Observaciones
								Si/No	Si/No	Software obsoleto/ No autorizado /	Aislamiento, Acceso restringido, Backups, etc		Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			
										Software obsoleto/ No autorizado /			Manual / Automatizado / Otro			

No.	Tipo de Dato / Información	Descripción	Clasificación	Área Responsable	Ubicación	Medidas de Protección	Plazo Mínimo - Máximo de Conservación
1	Datos Financieros	Información relacionada con ingresos, gastos, balances, compras, pagos, etc.	Confidencial	Delegación Administrativa	Equipo de cómputo de Delegada Administrativa	Acceso restringido, acceso interno	10 años como mínimo
2	Datos de Empleados	Información personal, historial laboral y detalles salariales de los empleados.	Confidencial	Delegación Administrativa	Equipo de cómputo del Jefe del Departamento de Recursos Humanos, Financieros y Materiales	Acceso restringido, acceso interno	10 años como mínimo
3	Datos de Proveedores	Nombres, direcciones, información de contacto e historial de compras de los clientes.	Confidencial	Delegación Administrativa	Equipo de cómputo de Delegada Administrativa	Acceso restringido, acceso interno	10 años como mínimo
4	Reportes de Metas	Información relacionada con el seguimiento y evaluación de objetivos institucionales o departamentales, incluyendo indicadores, avances y cumplimiento de metas.	Público/ Interno	Delegación Administrativa	Equipo de cómputo de Delegada Administrativa	Revisión periódica	10 años como mínimo
5	Manuales y políticas institucionales	Documentos que contienen lineamientos, procedimientos operativos, reglamentos internos y normas que rigen el funcionamiento de la institución.	Público/ Interno	Dirección de Riesgos, Políticas Públicas, Evaluación y Seguimiento	Equipo de cómputo de la Directora de Riesgos, Políticas Públicas, Evaluación y Seguimiento	Sólo lectura, acceso interno	N/A Solo se actualiza
6	Contenido Institucional de Divulgación Pública	Información para informar a la ciudadanía, incluyendo publicaciones en redes sociales, cobertura de eventos, boletines de prensa, campañas institucionales y material gráfico o audiovisual.	Público	Unidad de Vinculación y Comunicación Institucional	Equipo de cómputo de Jefa de la Unidad de Vinculación y Comunicación Institucional	Sólo lectura, acceso interno	10 años como mínimo

7	Información Sujeta a Transparencia y Acceso a la Información Pública	Documentación generada o administrada por el área de transparencia, incluyendo respuestas a solicitudes de acceso a la información, obligaciones de transparencia (art. 70 y 71 de la Ley General), versiones públicas de documentos oficiales y reportes solicitados.	Público / Confidencial (según el caso)	Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	Equipo de cómputo de la Jefa de la Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales		10 años como mínimo
8	Información de Control Interno y Cumplimiento Normativo	Documentación generada o administrada por el Órgano Interno de Control, que incluye declaraciones patrimoniales, actas de entrega-recepción, auditorías internas, informes de seguimiento y expedientes de responsabilidades administrativas.	Confidencial	Órgano Interno de Control	Equipo de cómputo y área del OIC		10 años como mínimo
9	Documentación Administrativa y de Archivo Institucional	Documentos que contienen oficios oficiales, inventarios documentales, expedientes en trámite, documentación en fase de concentración y transferencias documentales.	Confidencial / Interno / Público (según el contenido)	Dirección de Archivos	Equipo de cómputo y área de la Dirección de Archivos		10 años como mínimo
10	Datos relacionados con los Sistemas 1, 2 y 3 que conforman la Plataforma Digital Estatal	Documentación relacionada con los sistemas 1, 2 y 3 que conforman a la Plataforma Digital Estatal	Público / Confidencial (según el caso)	DSTPD	Servidor 10.1.1.1 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
11	Datos relacionados con los Sistemas 5 y 6 que conforman la Plataforma Digital Estatal	Documentación relacionada con los sistemas 5 y 6 que conforman a la Plataforma Digital Estatal	Público / Confidencial (según el caso)	DSTPD	Servidor 10.0.0.12 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo

12	Datos de la página web de la SESEA	Documentación que aloja la página web de la SESEA, normatividad, directorio institucional, organigrama, noticias, eventos, talleres, capacitaciones, etc	Público / Interno	DSTPD	Servidor 10.0.0.101 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
13	Datos del programa de el Banco de Buenas Prácticas	Datos que aloja la página del Banco de Buenas Prácticas	Público / Interno	DSTPD	Servidor 10.0.0.133 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
14	Datos del programa de Creciendo con Valores	Datos que aloja la página de Creciendo con valores	Público / Interno	DSTPD	Servidor 10.0.0.133 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
15	Datos del Tablero PEA	Información sobre las líneas de acción de la Política Estatal Anticorrupción	Público / Interno	DSTPD	Servidor 10.0.0.133 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
16	Datos del Tablero de la PDE	Información sobre el avance de Interconexión de los Sistemas (1,2,3,5 y 6), que conforman a la PDE	Público / Interno	DSTPD	Servidor 10.0.0.133 que se encuentra en Site.	Acceso restringido, acceso interno	10 años como mínimo
17	Datos Generales de la Empresa	Información pública sobre la empresa, como la misión, visión, comunicados, invitaciones y avisos.	Interno	Secretaría Técnica		Sólo lectura, acceso interno	10 años como mínimo

Bitácora de Eliminación de Datos

Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital

No.	Fecha de Eliminación	Tipo de Medio/Dispositivo	Ubicación	Tipo de Información Eliminada	Nivel de Sensibilidad	Método de Eliminación Aplicado	Formato del Dato	Plazo de retencion aplicado	Autorización de Eliminacion	Responsable de la Eliminación	Supervisor/ Validador	Observaciones
1	20/05/2025	Disco Duro SSD externo	Archivo General	Expedientes administrativos	Alta	Desmagnetización	Fisico/electronico	5 años		Juan Pérez (TI)	Laura Gómez (Auditoría)	Dispositivo fuera de uso
2	22/05/2025	USB 16 GB	Dirección Jurídica	Documentos internos borradores	Media	Sobrescritura con software (3 pasadas)	Fisico/electronico	5 años		Ana Ruíz (TI)	Pedro León (Jurídico)	Se reutilizará el USB
3	25/05/2025	Laptop institucional	Dirección de Sistemas	Informes operativos	Alta	Formateo seguro + sobrescritura	Fisico/electronico	3 años		Miguel Soto	Carla Reyes	Equipo dado de baja

Bitácora de Configuraciones Seguras

Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital

No.	Fecha	Dispositivo / Activo	Ubicación	Técnico Responsable	Cambio Realizado	Motivo del Cambio	Config. Respaldada	Validación por	Evidencia	Observaciones	Fecha proxima (si aplica)
1	20/05/2025	Router Cisco RV340	Sala de servidores	Carlos Mendoza	Deshabilitado Telnet, habilitado SSH, actualizado firmware	Endurecimiento de seguridad	Sí	Jefe de Departamento de la Direccion de Servicios Tecnologicos		Cumple política de acceso remoto seguro	
2	20/05/2025	Switch HP 2530-24G	Piso 2, área administrativa	Luis García	Deshabilitados puertos no usados, activado Port Security	Reducción de superficie de ataque	Sí	Analista de Plataforma Digital		Listo para revisión semestral	
3	20/05/2025	Firewall FortiGate 60F	Centro de Datos Principal	Mónica Torres	Aplicadas reglas de firewall, logs a SIEM	Revisión periódica de reglas	Sí	Jefe de Departamento de la Direccion de Servicios Tecnologicos		Actualización crítica completada con éxito	

Anexo F – Bitácora de Relación y Análisis de Equipos de la SESEA

Bitácora de relación y análisis de equipos de la SESEA													
Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital													
Núm.	Nombre del Equipo	Contraseña del Admin	IP Computadora	IP Telefono	Nombre del Responsable	Unidad	Fecha de revision	Evidencia de Seguridad	Evidencia Validación de Software	Evidencia de eliminacion de Sotware	Evidencia de Configuración de Suspención	Observaciones

Anexo G – Bitácora de Control de Acceso

Bitacora de control de Accesos

Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital

No.	Fecha	Tipo de Acción	Motivo	Nombre del Usuario	Usuario / Cuenta	Área / Sistema	Detalle de Acción	Responsable Aprobación	Evidencia Adjunta / Observación
1	10/05/2025	Alta de usuario	Nuevo Ingreso		j.santos@institucion.mx	Active Directory	Creación de usuario con acceso a carpetas compartidas de Finanzas	Jefe de Servicios Tecnologicos	Captura de alta en AD ✔ Checklist firmado ✔
2	11/05/2025	Modificación acceso	Cambio de area		l.rojas@institucion.mx	Sistema de Nómina	Permisos ampliados para ver reportes de pago	Director RH	Captura de permisos ✔ Solicitud firmada ✔
3	12/05/2025	Baja de usuario	Despido		m.gomez@institucion.mx	VPN / Correo institucional	Cuenta deshabilitada por baja laboral	DSTPD	Bitácora de baja ✔ Evidencia de revocación de acceso ✔
4	13/05/2025	Activación de MFA	N/A		admin.ad	Active Directory / VPN	Habilitación de MFA mediante app autenticadora	Analista DSTPS	Captura MFA ✔ Prueba de acceso MFA ✔
5	14/05/2025	Revisión Trimestral	N/A		Todos	Correo / Nube / Sistemas clave	Validación de accesos vigentes vs. solicitudes. MFA activo en cuentas administrativas	Auditor interno	Acta de revisión ✔ Informe de cumplimiento ✔
6	15/05/2025	MFA acceso remoto	N/A		j.martinez@institucion.mx	VPN	Confirmación de MFA para acceso remoto a VPN	Analista DSTPS	Captura de MFA en inicio de sesión ✔
7	15/05/2025	Inventario MFA	N/A		admin.db, admin.portal	SQL Server, Plataforma Web	Registro actualizado de cuentas administrativas con MFA habilitado	Analista DSTPS	Inventario MFA ✔ Capturas ✔
8	16/05/2025	Revisión SSO	N/A		Usuarios con SSO	Google Workspace / Azure AD	Validación de que SSO aplica MFA para acceso a servicios críticos	Responsable Infraestructura	Capturas de login con MFA ✔

Anexo H – Formato de Notificación de Alta, Baja o Cambio de Puesto
(Para uso de Recursos Humanos / Área Responsable)

Campo	Información
Fecha de notificación	[dd/mm/aaaa]
Nombre del empleado	[Nombre completo]
Correo institucional (si aplica)	[usuario@dominio]
CURP / ID interno (opcional)	[CURP o número de empleado]
Área o departamento	[Ej. Dirección Jurídica]
Puesto actual / nuevo puesto	[Ej. Coordinador de Contratos]
Tipo de solicitud	☐ Alta de nuevo empleado ☐ Baja de empleado ☐ Cambio de puesto o funciones
Fecha efectiva del cambio o baja	[dd/mm/aaaa]
¿Requiere revocar todos los accesos?	☐ Sí☐ No (especificar abajo)
Observaciones / Acciones específicas requeridas	[Ej. Transferir correos, respaldo de carpeta, etc.]
Solicitante (nombre y cargo)	[Ej. Lic. Karla Mendoza – Jefa de Recursos Humanos]
Firma del solicitante	_____

Bitácora de Eventos Auditables y Gestión de Registros

Departamento de Tecnología / Servicios Tecnológicos y Plataforma Digital

No.	Activo / Sistema	Tipo de Evento Registrado	Ubicación del Log	Capacidad actual del Log	Tiempo de Retención	Responsable de Revisión	Frecuencia de Revisión
1	Servidor de archivos	Inicio/Cierre de sesión, acceso a carpetas sensibles	/var/log/audit.log (Linux)		2 años	DSTPD - Auditoría	Trimestral
2	Firewall FortiGate	Cambios en configuración, bloqueos, alertas	SIEM Central		1 año	DSTPD	Mensual
3	Base de Datos PostgreSQL	Consultas sensibles, intentos fallidos	log/postgres.log		1 año	DBA	Trimestral
4	Sistema ERP	Cambios críticos, errores del sistema	/erp/logs/audit.log		2 años	Encargado de ERP	Semestral

Anexo J – Bitácora de Incidencias de Seguridad

BITÁCORA DE INCIDENCIAS DE SEGURIDAD														
Dirección de Servicios Tecnológicos y Plataforma Digital														
Número de Incidente	Fecha de Detección	Responsable que Registra	Usuario Responsable	Cargo / Área de Adscripción	Tipo de Dispositivo	Marca / Modelo	Número de Serie / Inventario	Conectado a Red Institucional (Sí/No)	Acceso a Sistemas Críticos (Especificar)	Descripción Detallada	Presencia de Información Confidencial (Sí/No)	Acción Implementada

Anexo K – Inventario Técnico Institucional

INVENTARIO TÉCNICO INSTITUCIONAL

ID Activo	Número de Inventario	Usuario Asignado	Cargo	Área	Tipo de Equipo	Marca / Modelo	Número de Serie	Responsable Técnico	Documento de Aceptación Firmado (Sí/No)	Fecha Firma Usuario	Observaciones

T R A N S I T O R I O S

Único.- El presente Acuerdo entrará en vigor a partir de la fecha de su aprobación.

El presente Manual de Protocolos y Políticas en Materia de Ciberseguridad de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, fue aprobado en la Primera Sesión Ordinaria 2026, por unanimidad de votos de las personas que estuvieron presentes y que integran el Comité Coordinador del Sistema Estatal Anticorrupción y Órgano de Gobierno de la Secretaría Ejecutiva del mismo sistema, ciudadanos, C.P. Lizet Esperanza García Torres, Auditora Especial de Normatividad, en suplencia por ausencia del C.P. Marco Antonio Bravo Pantoja, Auditor Superior de Michoacán; Mtra. Marisol Sánchez Zamudio, Fiscal Especializada en Combate a la Corrupción; Lic. Francisco Ramírez Flores, Titular de la Secretaria de Contraloría del Estado; Dra. Laura Elena Alanís García, Magistrada Presidenta Sustituta del Poder Judicial del Estado; Mtra. Azucena Marín Correa, Magistrada de la Quinta Sala del Tribunal en materia Anticorrupción y Administrativa del Estado de Michoacán, en representación de la Magistrada Presidenta, la Dra. Lizett Puebla Solórzano; L.A. Oscar Chávez Arriaga, Contralor Municipal de Epitacio Huerta; Lic. María Monserrat Farías Aguirre, Contralora Municipal de Ziracuaretiro; y L.E. Rubén Alejandro García Alcántar, Contralor Municipal de Tangamandapio. Se emite la presente, en términos de lo dispuesto por el artículo 37, fracciones I, II, III y VI de la Ley del Sistema Estatal Anticorrupción para el Estado de Michoacán de Ocampo.

Dra. Miryam Georgina Alcalá Casillas,
Secretaria Técnica de la Secretaría Ejecutiva
del Sistema Estatal Anticorrupción de Michoacán.

SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN