# Politicas y Estandares de Seguridad Informatica

Secretaría Anticorrupción y Buen Gobierno
Dirección General de Control de Tecnologías de la Informacion y Comunicación

**Nota de Revisión**
**Elaborado por:** Ing. Samara Abigail Beltrán Encinas
**Revisado por:** Ing. Karina Lerma Gonzalez
**Versión del Documento:** 1.0
**Última Actualización:** marzo de 2025

# Contenido

# Introducción

La necesidad de prestar servicios más eficientes ha convertido a nuestros activos de información y equipos informáticos en recursos vitales. La adecuada utilización y disponibilidad de estos recursos son esenciales para mejorar la eficacia y eficiencia de nuestras operaciones. Por lo tanto, es nuestro deber preservar, utilizar y mejorar estos activos. Para garantizar la protección de la información y los sistemas informáticos contra diversas amenazas y riesgos, como el fraude, el sabotaje y el espionaje, es fundamental contar con políticas de seguridad informática que regulen nuestras actividades relacionadas con los sistemas de información.

# Objetivo del Manual

El objetivo principal de este manual es establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal. Estas políticas son fundamentales para garantizar la protección de nuestros activos de información y sistemas informáticos, y para promover un entorno de trabajo seguro y eficiente.

# Alcance

Este documento define las Normas y Políticas de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos.

# Sanciones por Incumplimiento

El incumplimiento de este manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

# 1. Políticas y Estándares de Seguridad Informática

## 1.1 Protección de Sistemas de Comunicaciones

- Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada para evitar el acceso físico directo de los usuarios.
- El acceso de terceras personas debe ser identificado, controlado y vigilado durante su estancia.
- Las visitas internas o externas podrán acceder a las áreas restringidas solo si están acompañadas por un responsable del área de tecnología de sistemas de información y en el horario establecido.

## 1.2 Resguardo y Protección de la Información

### *Portales y Sistemas:*

La Secretaría Anticorrupción y Buen Gobierno establece políticas claras para el resguardo y protección de la información crítica contenida en sus portales y sistemas institucionales. Se utiliza un equipo de almacenamiento dedicado exclusivamente a la realización de respaldos, gestionado por el Centro de Datos de Gobierno Digital.

- Los respaldos se realizan periódicamente, asegurando la disponibilidad e integridad de los datos.

- Los respaldos son monitoreados continuamente, con alertas automatizadas para notificar cualquier inconsistencia o fallo.
- La Dirección General de Infraestructura y Conectividad de la Subsecretaría de Gobierno Digital de Oficialia Mayor, es responsable de la programación, ejecución y verificación de los respaldos.

*Unidades:*

- **Identificación de Información Crítica:** Los usuarios deben identificar la información crítica que debe ser respaldada y almacenarla según su nivel de clasificación.
- **Reporte de Riesgos:** Los usuarios deben reportar de inmediato cualquier riesgo real o potencial para equipos de cómputo o comunicaciones a la Dirección General de Control de Tecnologías de la Información y Comunicaciones.
- **Protección de Dispositivos:** Los usuarios deben proteger memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles, incluso si no se utilizan y contienen información reservada o confidencial.
- **Evitar la Fuga de Información:** Los usuarios deben evitar en todo momento la fuga de información almacenada en los equipos de cómputo asignados.

## 1.3 Infraestructura

### Estándares de Cableado Estructurado

- Durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes, se deben considerar los estándares vigentes de cableado estructurado.

### Aprobación de Equipos de TI

- Todo equipo de TI debe ser revisado, registrado y aprobado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional.
- Las unidades administrativas deben desconectar dispositivos no aprobados y reportar estas conexiones como incidentes de seguridad.

### Mantenimiento de Redes

- La Dirección General de Control de Tecnologías de la Información y Comunicaciones debe asegurar que las labores de mantenimiento de redes de voz y datos sean realizadas por personal idóneo y autorizado.
- Deben llevar un control de la programación de los mantenimientos preventivos.

### Conectividad a Internet

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida, utilizando el sistema de seguridad con Firewall incorporado.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio.
- Todas las actividades en Internet deben estar relacionadas con tareas y actividades laborales.

## Red Inalámbrica (WIFI)

### *Definición de la Red Inalámbrica*

- La red inalámbrica permite la conexión a la red de Datos e Internet de la Secretaría Anticorrupción y Buen Gobierno sin necesidad de cables.

### *Condiciones de Uso*

- Estas condiciones se aplican a todos los dispositivos de comunicación inalámbrica, como computadoras portátiles y tabletas, con capacidad de conexión Wireless.

### *Tecnología Utilizada*

- La red inalámbrica utiliza el estándar 802.11b/g/n con cifrado WPA2.

### *Compatibilidad de Tarjetas de Red Inalámbrica*

- Las tarjetas de red inalámbrica deben cumplir con la certificación Wi-FiTM y ser compatibles con los requerimientos descritos.

### *Cobertura*

- La cobertura de la red inalámbrica está sujeta a diversos factores, por lo que no se garantiza el acceso desde cualquier punto fuera de la cobertura de la Secretaría.

### *Protocolo Soportado*

- La red inalámbrica solo admite el protocolo TCP/IPV.4.

### *Restricciones y Prohibiciones*

- Se prohíbe la operación no autorizada de "puntos de acceso" y la configuración de tarjetas inalámbricas como "puntos de acceso."

### *Administración de la Red Inalámbrica*

- La administración, habilitación y desactivación de usuarios en la red inalámbrica es responsabilidad de la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

### *Identificación y Activación de Usuarios*

- Los solicitantes deben ser empleados de la Secretaría.
- El registro de usuarios se realiza a través de la Mesa de Ayuda, presentando el dispositivo que se conectará a la red inalámbrica.
- Es obligatorio registrar la dirección MAC de las tarjetas inalámbricas de todos los dispositivos institucionales.
- Los usuarios deben utilizar autenticación WPA2, con nombres de usuario y contraseñas que cambian periódicamente.
- La Dirección General de Control de Tecnologías de la Información y Comunicaciones lleva un registro de los eventos de conexión para garantizar el uso adecuado de los recursos de red.
- Se prohíbe el uso de programas que recolecten paquetes de datos de la red inalámbrica.
- Los usuarios deben comunicar cualquier cambio en los equipos registrados a la Mesa de Ayuda.

### *Restricciones y Prohibiciones de Acceso a Internet*

- Se prohíbe el uso de programas para compartir archivos (Peer to Peer).
- Se prohíbe el acceso a páginas con contenido explícito de pornografía.
- No se permite el uso de sitios de videos en línea o en tiempo real.
- Los juegos "online" están prohibidos.
- No está permitido el ingreso de equipos celulares personales.

**Excepciones: Situaciones Especiales y Acceso de Invitados**

### *Configuración de Seguridad*

- Se han implementado medidas de seguridad que restringen ciertas palabras y sitios web. Los usuarios pueden notificar a la Mesa de Ayuda si encuentran acceso denegado a sitios inofensivos.

### *Eventos Especiales*

- Para eventos, cursos, talleres, conferencias, etc., se pueden habilitar equipos con acceso a la red inalámbrica temporalmente, presentando una solicitud con al menos dos días hábiles de anticipación.

### *Anulación Temporal de Restricciones*

- Durante eventos especiales, las restricciones de acceso pueden ser anuladas temporalmente a solicitud expresa y con aviso de al menos dos días hábiles.

### *Acceso de Invitados*

- La red inalámbrica de Invitados permite a los usuarios utilizar los servicios de Internet en áreas de cobertura de la Secretaría.
- Los usuarios invitados no tienen acceso a la Red directa de la institución ni a ningún recurso privado.
- Esta red utiliza un Portal Cautivo y las contraseñas se actualizan cada 6 meses.

## 1.4 Protección y Ubicación de los Activos Tecnológicos

### *Responsabilidad del Usuario*

- Cada estación de trabajo, dispositivo móvil y recurso tecnológico está asignado a un usuario, quien es responsable de su uso adecuado y eficiente.

### *Movimiento y Reubicación de Equipos*

- Los usuarios no deben mover, reubicar, instalar, desinstalar dispositivos ni retirar sellos de los equipos sin autorización previa de la Mesa de Ayuda. Cualquier necesidad de este tipo debe ser solicitada a través de la Mesa de Ayuda.

### *Capacitación para el Uso de Herramientas Informáticas*

- Los usuarios deben solicitar y recibir la capacitación necesaria para el manejo adecuado de las herramientas informáticas en sus equipos para evitar riesgos por un uso incorrecto y aprovechar al máximo estas herramientas.

### *Almacenamiento de Información*

- La información debe almacenarse exclusivamente en el directorio de trabajo asignado a cada usuario, ya que los otros directorios están destinados a archivos de programas y sistema operativo.

### *Cuidado del Entorno de Trabajo*

- No se permite consumir alimentos ni líquidos mientras se opera el equipo de cómputo, excepto en botellas de plástico.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.
- El entorno donde se ubica el equipo informático debe mantenerse limpio y libre de humedad.
- Se debe evitar pisar o aplastar los cables de conexión con otros objetos.

### *Mantenimiento y Garantía*

- Queda prohibido a los usuarios abrir o desarmar los equipos de cómputo, ya que esto invalidaría la garantía proporcionada por el proveedor.
- La Mesa de Ayuda es la única autorizada para la instalación, cambio o eliminación de componentes en la plataforma tecnológica.

### *Configuración de Recursos Tecnológicos*

- La Dirección General de Control de Tecnologías de la Información y Comunicaciones debe establecer configuraciones adecuadas para los recursos tecnológicos para preservar la seguridad de la información y garantizar un uso apropiado.

### *Entrega de Estaciones de Trabajo*

- La Dirección General de Control de Tecnologías de la Información y Comunicaciones es responsable de preparar y entregar las estaciones de trabajo fijas y portátiles a los funcionarios.

### *Restricciones en Dispositivos*

- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos institucionales asignados.
- Los usuarios no deben modificar las configuraciones de seguridad ni desinstalar el software proporcionado en los dispositivos institucionales entregados.

## 1.5 Mantenimiento de Activos Informáticos e Infraestructura

### *Personal Autorizado para el Mantenimiento*

- El personal autorizado designado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones será responsable de brindar servicios de mantenimiento preventivo y correctivo a los activos informáticos y la infraestructura.
- Los usuarios deben solicitar la identificación del personal autorizado antes de permitir el acceso para el mantenimiento.

### *Mantenimiento Preventivo*

- El período para llevar a cabo el mantenimiento preventivo será determinado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

### *Restricciones de Mantenimiento*

- Está estrictamente prohibido dar mantenimiento a equipos de cómputo que no sean propiedad de la Secretaría.
- Cualquier mantenimiento correctivo requerido debe solicitarse a través de la Mesa de Ayuda.

### *Reparación y Tiempo de Reparación*

- El tiempo de reparación dependerá del nivel de daño o tipo de problema presentado en el equipo.
- En caso necesario, se enviará a reparación especializada fuera de la Secretaría.

### *Respaldo de Información*

- Los usuarios deben asegurarse de respaldar la información relevante antes de enviar el equipo a reparación.
- También deben borrar información sensible que se encuentre en el equipo para prevenir la pérdida involuntaria de datos, solicitando asesoría al personal de la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

## 1.6 Pérdida o Transferencia de Equipo

### *Responsabilidad del Usuario*

- El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia.
- Responderá por dicho bien de acuerdo con la normatividad vigente en caso de robo, extravío o pérdida.

### *Resguardo para Laptops*

- El resguardo de las laptops es personal e intransferible, por lo que queda prohibido su préstamo.

### *Reporte de Pérdida o Extravío*

- El usuario debe informar inmediatamente a la Dirección General de Administración y Control Presupuestal en caso de desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- Dicha Unidad Administrativa debe notificar a la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

## 1.7 Daño del Equipo

### *Causas de Daño*

- El equipo de cómputo o cualquier recurso de tecnología de información que sufra daños debido a maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.
- Se determinará la causa de la descompostura en cada caso.

# 2. Políticas, Estándares de Seguridad y Administración de Operaciones de Cómputo

## Política de Protección de la Información

- Los usuarios deben utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Secretaría Anticorrupción y Buen Gobierno.
- Deben proteger la información reservada o confidencial que deba ser almacenada o transmitida, ya sea dentro de la red interna de la Secretaría o hacia redes externas como internet.
- Los usuarios deben conocer y aplicar medidas para la prevención de código malicioso, como virus, malware o spyware, y pueden solicitar asesoría a la Mesa de Ayuda.

## 2.1 Uso de Medios de Almacenamiento

### *Respaldo de Información*

- Los usuarios deben respaldar periódicamente la información sensible y crítica en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la Mesa de Ayuda para determinar el medio de respaldo adecuado.

### *Conservación de Registros*

- Los servidores públicos deben conservar registros e información activa, así como información clasificada como reservada o confidencial, de acuerdo con las disposiciones la Ley General de Transparencia y Acceso a la Información Pública y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

### *Registro y Auditoría*

- Las actividades realizadas por los usuarios en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

### *Uso de Medios de Almacenamiento Personales*

- El personal de la Secretaría y el personal proporcionado por terceros no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Dependencia.

## 2.2 Instalación de Software

### *Acceso a Proveedores para Actualizaciones*

- La Dirección General de Control de Tecnologías de la Información y Comunicaciones otorgará accesos temporales y controlados a los proveedores para realizar actualizaciones de software y supervisará estas actualizaciones.

### *Validación de Riesgos en Actualizaciones de Software Operativo*

- Se validará el riesgo que conlleva la migración hacia nuevas versiones del software operativo.
- Se garantizará el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica al actualizar el software operativo.

### *Software Precargado en la Adquisición de Equipo de Cómputo*

- En la adquisición de equipo de cómputo, se incluirá el software vigente precargado con su licencia correspondiente.

### *Autorización para Instalar Software No Propiedad de la Secretaría*

- Los usuarios que necesiten instalar software que no sea propiedad de la Secretaría deberán justificar su uso y solicitar autorización a la Dirección General de Control de Tecnologías de la Información y Comunicaciones a través de la Mesa de Ayuda.
- Deberán indicar el equipo de cómputo donde se instalará el software y el período de instalación.
- La instalación está sujeta a la presentación de la factura de compra del software.
- Si el dueño del software no presenta la factura de compra, se procederá a desinstalar el software de inmediato.

### *Prohibición de Instalar Software No Autorizado*

- Queda prohibido que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo o cualquier equipo conectado a la red de la Secretaría que no esté autorizado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

### *Propiedad del Software de la Secretaría*

- Todo programa o sistema adquirido por compra, donación o cesión es propiedad de la Secretaría.
- Los sistemas informáticos desarrollados con los recursos de la Dirección se mantendrán como propiedad de la Secretaría respetando la propiedad intelectual correspondiente.
- Se propiciará la gestión de patentes y derechos de creación de software propiedad de la Secretaría.
- La Dirección administrará las licencias de software y vigilará su vigencia.

## 2.3 Identificación de Incidente

### *Reporte de Incidentes*

- Los usuarios que sospechen o tengan conocimiento de un incidente de seguridad informática deberán reportarlo a la Dirección lo antes posible.
- Deberán proporcionar detalles claros sobre por qué consideran que es un incidente de seguridad informática.

### *Revelación de Información Confidencial o Reservada*

- Cuando se sospeche o tenga conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin autorización, el usuario informático notificará al titular de su adscripción.

### *Reporte de Cualquier Incidente*

- Cualquier incidente durante la utilización de activos de tecnología de información debe ser reportado a la Dirección.

## 2.4 Controles contra Código Malicioso

### *Enfoque Integral de Seguridad*

- Se debe aplicar un enfoque integral que involucre controles humanos, técnicos y administrativos para mitigar los riesgos asociados con el software malicioso y las técnicas de hacking.

### *Protección con Software Antivirus*

- Todas las estaciones de trabajo deben estar protegidas con software antivirus que tenga capacidad de actualización automática en cuanto a firmas de virus.

### *Herramientas de Protección Proporcionadas por la Dirección General*

- La Dirección General de Control de Tecnologías de la Información y Comunicaciones proporcionará herramientas como antivirus, antimalware, antispam, antispyware, entre otras, para reducir el riesgo de infección de software malicioso y garantizar la seguridad de la información.

### *Seguimiento del Tráfico de Red*

- Se realizará seguimiento al tráfico de red cuando se detecten actividades inusuales en el rendimiento.

### *Licencias de Software de Seguridad*

- El software de seguridad, como antivirus, antimalware, antispam y antispyware, debe contar con las licencias de uso necesarias y estar actualizado regularmente con las últimas bases de datos de firmas del proveedor de servicios.

### *Escaneo Regular de Información*

- La información almacenada en la plataforma tecnológica debe ser escaneada por el software de antivirus al menos una vez a la semana, incluyendo la información transmitida a través del correo electrónico.

### *Restricción de Cambios en la Configuración*

- Los usuarios y personal externo no pueden realizar cambios en la configuración del software de seguridad, como antivirus, antispyware, antispam y antimalware.

### *Ejecución de Software de Seguridad*

- Los usuarios deben ejecutar el software de seguridad sobre archivos y documentos que se abren o ejecutan por primera vez, especialmente aquellos de medios de almacenamiento externos o correos electrónicos.

### *Origen Seguro de Archivos Adjuntos*

- Los usuarios deben asegurarse de que los archivos adjuntos de correos electrónicos descargados de Internet o de medios de almacenamiento provengan de fuentes conocidas y seguras para evitar infecciones de virus informáticos o instalación de software malicioso.

### *Reporte de Infecciones o Sospechas*

- Los usuarios que detecten o sospechen de infecciones por software malicioso deben notificar a la Mesa de Ayuda para tomar las medidas de control adecuadas.

### *No Intentar Eliminar Virus por Cuenta Propia*

- Los usuarios no deben intentar eliminar virus de las computadoras por sí mismos; en su lugar, deben llamar a la Mesa de Ayuda para su atención.

### *Consecuencias del Uso no Aceptable*

- El uso no aceptable resultará en la cancelación de cuentas o desconexión temporal o permanente, según las políticas. La reconexión se realizará cuando se considere que el uso no aceptable se ha suspendido.

## 2.5 Atención a Usuarios de Servicios Tecnológicos

Garantizar una atención eficiente y de calidad a los usuarios de servicios tecnológicos proporcionados por la Dirección General de Control de Tecnologías de la Información y Comunicaciones de la Secretaría Anticorrupción y Buen Gobierno.

### *Procedimientos y Responsabilidades*

- **Registro de Incidencias:** Los usuarios deben reportar cualquier incidencia en el uso de servicios tecnológicos, las cuales serán registradas a través del sistema de Mesa de Ayuda. Los reportes pueden realizarse mediante llamadas telefónicas, correos electrónicos, atención presencial u oficios.

- **Soporte Telefónico:** La Mesa de Ayuda ofrece soporte telefónico para resolver dudas operativas y funcionales relacionadas con aplicaciones y sistemas operativos. El horario de atención es de 8:00 a.m. a 4:00 p.m.

- **Acceso Remoto:** Se utilizará la herramienta de Acceso Remoto para brindar asistencia en tiempo real, adaptándose a las necesidades y problemáticas del usuario.

- **Soporte en Sitio o Remoto:** El especialista de la Mesa de Ayuda decidirá si el soporte se proporciona de forma remota o en sitio, considerando la gravedad del problema y la disponibilidad de recursos.

- **Canalización de Solicitudes:** Las solicitudes que requieran la intervención de otras áreas serán canalizadas de inmediato. Se informará al usuario sobre esta decisión.

- **Norma ISO-9001:2008:** Para proporcionar estos servicios, seguimos un procedimiento documentado bajo la norma ISO-9001:2008. Puede consultar este procedimiento, denominado "P02 Mesa de Ayuda tecnológica", en la página https://sicad.sonora.gob.mx.

- **Confidencialidad:** Debido a la naturaleza confidencial de la información a la que se accede en el soporte técnico, el personal de la Dirección General de Control de Tecnologías de la Información y Comunicaciones debe seguir códigos de ética, normas y procedimientos establecidos.

- **Atribuciones de Ingenieros de Soporte:** Los Ingenieros de Soporte tienen varias responsabilidades, incluyendo:

    - Acceso remoto a computadoras solo con autorización explícita del propietario.

    - Uso de analizadores previa autorización y supervisión del usuario.

    - Actualización del inventario de equipos y auditoría periódica de sistemas y servicios de red sin previo aviso.

    - Reporte de incidentes de seguridad y formación continua en tecnología, seguridad informática, ética y comunicación.

# 3. Políticas y Estándares de Controles de Acceso Lógico

## Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado, lo cual incluye su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica de la Secretaría Anticorrupción y Buen Gobierno. Por lo tanto, cada usuario debe mantener esta información de forma estrictamente confidencial.

## 3.1 Administración y Uso de Contraseñas

Garantizar una adecuada administración y uso de contraseñas para acceder a la información y la infraestructura tecnológica de la Secretaría Anticorrupción y Buen Gobierno.

### *Procedimientos y Responsabilidades*

- **Autenticación Obligatoria:** Todos los usuarios deben autenticarse a través de los mecanismos de control de acceso proporcionados por la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

- **Confidencialidad de Contraseñas:** Los usuarios no deben compartir sus identificadores de usuario ni contraseñas, ya que serán responsables de cualquier actividad realizada con estos identificadores y contraseñas, a menos que demuestren que les fueron usurpados.

- **Asignación Individual de Contraseñas:** Queda prohibido el uso de contraseñas compartidas, y la asignación de contraseñas para el acceso a la red y sistemas debe hacerse de forma individual.

- **Procedimiento para Olvido o Bloqueo de Contraseña:** Cuando un usuario olvide, bloquee o extravíe su contraseña, debe informarlo a la Mesa de Ayuda de la Dirección General de Control de Tecnologías de la Información y Comunicaciones. Se debe especificar si se trata de la contraseña de acceso a la red o a sistemas desarrollados por la Dirección.

- **Obtención o Cambio Seguro de Contraseña:** La obtención o el cambio de una contraseña debe realizarse de manera segura, y el usuario debe acreditarse ante la Dirección General de Control de Tecnologías de la Información y Comunicaciones como empleado de la Secretaría Anticorrupción y Buen Gobierno.

- **Restricción de Visibilidad de Contraseñas:** Las contraseñas no deben estar visibles en ningún medio impreso o escrito en el área de trabajo del usuario de manera que personas no autorizadas puedan acceder a ellas.

- **Requisitos de Contraseñas:** Las contraseñas deben cumplir con ciertos requisitos de seguridad, como contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

- **Cambio de Contraseña por Requerimiento:** Los usuarios tienen el derecho de cambiar su contraseña cuando lo necesiten.

- **Cambio de Contraseña en Caso de Sospecha:** Si un usuario sospecha que otra persona conoce su contraseña, está obligado a cambiarla de inmediato.

- **Almacenamiento de Contraseñas:** Los usuarios no deben almacenar sus contraseñas en programas o sistemas que permitan esta facilidad.

## 3.2 Equipo Desatendido

Garantizar la seguridad de los equipos de cómputo cuando los usuarios necesiten ausentarse de sus escritorios.

### *Procedimientos y Responsabilidades*

- **Controles de Acceso Obligatorios:** Los usuarios deben mantener sus equipos de cómputo protegidos con controles de acceso, como contraseñas y protectores de pantalla, previamente instalados y autorizados por la Dirección General de Control de Tecnologías de la Información y Comunicaciones, cuando se ausenten de sus escritorios por un tiempo.

## 3.3 Control de Accesos Remotos

Establecer reglas para el acceso a redes externas y la administración remota de equipos conectados a internet.

### *Procedimientos y Responsabilidades*

- **Prohibición de Acceso no Autorizado:** Se prohíbe el acceso a redes externas a través de cualquier dispositivo no autorizado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

- **Administración Remota con Autorización:** La administración remota de equipos conectados a internet solo está permitida cuando se cuenta con autorización y se utiliza un mecanismo de control de acceso seguro, como una VPN, autorizado por la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

## 3.4 Revisiones del Cumplimiento

Realizar revisiones y controles para verificar el cumplimiento de las políticas y estándares de seguridad informática.

### *Procedimientos y Responsabilidades*

- **Verificación del Cumplimiento:** La Dirección General de Control de Tecnologías de la Información y Comunicaciones llevará a cabo acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

- **Mecanismos de Control de Uso de Recursos:** La Dirección General de Control de Tecnologías de la Información y Comunicaciones podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que se detecte será reportado conforme a lo indicado en la Política de Seguridad del Personal.

## 3.5 Violaciones de Seguridad Informática

Establecer normas para prevenir violaciones de seguridad informática y definir las acciones prohibidas.

### *Procedimientos y Responsabilidades*

- **Prohibición de Herramientas de Violación de Seguridad:** Queda terminantemente prohibido el uso de herramientas de hardware o software con la intención de violar los controles de seguridad informática, a menos que se cuente con autorización expresa de la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

- **Pruebas de Controles con Autorización:** No se permite realizar pruebas de controles de seguridad informática en los elementos de Tecnología de la Información sin la aprobación previa de la Dirección General de Control de Tecnologías de la Información y Comunicaciones.

- **Prohibición de Introducir Código Malicioso:** Está estrictamente prohibido crear, introducir o propagar cualquier tipo de código, como virus, malware, spyware, u otros, diseñados para replicarse, dañar o afectar el desempeño de las computadoras, redes e información de la Secretaría Anticorrupción y Buen Gobierno.

- **Sanciones por Infracciones:** Cualquier infracción a las políticas de seguridad informática será sancionada de acuerdo con lo que dispone la Ley de Responsabilidades de los Servidores

Públicos del Estado y de los Municipios cuando se comprometa la seguridad de la Red institucional.

# 4. Disposiciones Generales

## Proceso de Revisión y Actualización

Este Manual de Políticas y Estándares de Seguridad Informática estará sujeto a un proceso regular de revisión y actualización, el cual será responsabilidad de la Dirección General de Control de Tecnologías de la Información y Comunicaciones. Las revisiones se llevarán a cabo al menos una vez al año o cuando ocurran cambios significativos en la organización, como el aumento en el número de empleados, modificaciones en la infraestructura informática o la implementación de nuevos servicios.

## Fecha de Entrada en Vigor

Este Manual entrará en vigor a partir de su autorización y deberá ser ampliamente difundido en todas las áreas de la organización para su conocimiento y aplicación.

# 5. Glosario

- **Acceso físico:** Ingreso a áreas físicas o instalaciones donde se encuentran recursos tecnológicos.
- **Antivirus:** Software diseñado para detectar y eliminar virus informáticos.
- **Cifrado:** Proceso de convertir datos en un formato ilegible para proteger su confidencialidad.
- **Firewall:** Sistema de seguridad que controla el tráfico de red y previene intrusiones no autorizadas.
- **Intrusión:** Acceso no autorizado a sistemas o redes.
- **Malware:** Término genérico para programas maliciosos como virus, spyware y troyanos.
- **Política de contraseñas:** Directrices para crear y mantener contraseñas seguras.
- **Respaldos:** Copias de seguridad de datos y sistemas para la recuperación en caso de fallos.
- **Software de seguridad:** Programas que protegen contra amenazas como virus y malware.
- **Seguridad de red:** Medidas para proteger la integridad y confidencialidad de la información transmitida por redes.
- **Phishing:** Intento de engañar a las personas para obtener información confidencial, como contraseñas.
- **Actualización de software:** Mantener el software actualizado para corregir vulnerabilidades.
- **Autenticación:** Verificación de la identidad del usuario antes de conceder acceso.
- **Código malicioso:** Programas diseñados para causar daño o robar información.
- **Vulnerabilidad:** Debilidad en sistemas o software que podría ser explotada por atacantes.
- **Acceso remoto:** Conexión a sistemas desde ubicaciones externas a través de redes seguras.

- **Incidente de seguridad:** Evento que pone en riesgo la confidencialidad o integridad de la información.
- **Respaldo de datos:** Copia de seguridad de información crítica para su recuperación en caso de pérdida.
- **Control de acceso:** Mecanismos para autorizar y autenticar el acceso a recursos tecnológicos.
- **Seguridad física:** Protección de equipos y activos tecnológicos en instalaciones físicas.