1.

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIÓN, PARA EL H. AYUNTAMIENTO DE SAN FELIPE TEPATLÁN, PUEBLA

2021-2024

SAN FELIPE TEPATLÁN
Construir y Transformar

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIÓN, PARA EL H. AYUNTAMIENTO DE SAN FELIPE TEPATLÁN, PUEBLA.

CLAVE: 23/09

AUTORIZACIONES

ING. ANTONIO MARQUEZ ZARAGOZA PRESIDENTE MUNICIPAL **AUTORIZA**	**C. HERMENEGILDO DE LA SOTA CRUZ** CONTRALOR MUNICIPAL **ELABORA Y APRUEBA**	**LIC. FILIBERTO LUCAS LOPEZ** SECRETARIO GENERAL **AUTORIZA**
ING. ANTONIO MARQUEZ ZARAGOZA	**C. HERMENEGILDO DE LA SOTA CRUZ**	**LIC. FILIBERTO LUCAS LOPEZ**

PRESIDENTE MUNICIPAL **AUTORIZA**	CONTRALOR MUNICIPAL **ELABORA Y APRUEBA**	SECRETARIO GENERAL **AUTORIZA**

Hoja de Edición:

Aprobado por cabildo de fecha 27 de marzo de 2022, con fundamento en los artículos, 169 fracciones VII y IX de la Ley Orgánica Municipal.

1. INTRODUCCIÓN

1.1. Alcance y Función del Manual

Este documento es elaborado por el área de Contraloría Municipal del Honorable Ayuntamiento de San Felipe Tepatlán, Puebla. Las políticas y lineamientos aplican para su aplicación por todas las áreas que hagan uso de Sistemas Informáticos.
Estos sistemas incluyen las redes de área local, las computadoras personales (PC), radios de comunicación y demás sistemas administrativos.

1.2. Asesoramiento y Guía

Se puede obtener asesoramiento y guía respecto a los controles, procedimientos y las técnicas de seguridad informática en el área de Contraloría Municipal.

2. POLÍTICA DE SEGURIDAD INFORMÁTICA

2.1. Definición Técnica

La Seguridad Informática implica la protección de la información en términos de:

a) **Confidencialidad**: divulgar información sólo a las personas y los procesos autorizados;
b) **Integridad**: garantiza la exactitud e integridad de la información.
c) **Disponibilidad**: asegura el acceso y la utilización oportunos de la información y los sistemas de información como se requiera, y la protección de los equipos, software y demás activos de tecnología informática.

2.2. Alcance

Esta política se aplica a todos los servidores públicos, empleados, sistemas informáticos, software, documentación o información, equipos y demás recursos de Tecnologías de la Información.

2.3 Inventario de activos

Se debe llevar un inventario centralizado y actualizado de los recursos de Tecnología de Información del H Ayuntamiento, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan.

2.4 Uso Aceptable de Activos

Todos los servidores públicos, empleados y terceras partes son responsables de seguir las reglas existentes para el buen uso de la información y activos asociados con el procesamiento de dicha información.

Se debe contar con un procedimiento de restauración y resguardo de información para el uso aceptable de los activos de información.

2.5. Clasificación de la información.

Los activos informáticos deben estar clasificados con base al impacto que representan en el H. Ayuntamiento y además en sus propiedades de seguridad como confidencialidad, disponibilidad e integridad.

2.6. Etiquetado y Manejo de la Información

Toda la información que se encuentre almacenada en papel o medios magnéticos y ópticos, se debe etiquetar indicando su tipo de clasificación para facilitar su control, manejo y cuidado por parte del personal.

2.7. Administración de Riesgos

Todo el personal que haga uso de sistemas informáticos debe generar una matriz de riesgos para sus activos de información.
El objetivo principal de la administración de riesgos es de disminuir el impacto de los eventos potenciales que pueden afectar el alcance de los objetivos del H, Ayuntamiento.
Los controles de Seguridad Informática deben integrarse en una matriz donde se considere el costo de inversión, costo de operación y valor de la información a resguardar y demás activos en riesgo, considerando el riesgo por el daño que pudiera derivar de las violaciones potenciales de la seguridad, así como la trazabilidad de riesgo.

2.8. Responsabilidades Administrativas

El área de Contraloría Municipal debe determinar las responsabilidades explícitas para implementar, operar y administrar los controles de Seguridad Informática.

2.9. Disciplina Interna

Las políticas y lineamientos de Seguridad Informática deben cumplirse en todo momento.

2.10. Capacitación del Personal en materia de Seguridad de la Información

La Contraloría Municipal debe considerar en su plan de trabajo el proporcionar a los servidores públicos y empleados responsables de Tecnologías de la Información y Comunicaciones, programas de concientización, educación y capacitación adecuados en función de las necesidades.

El personal debe recibir capacitación periódica (1 vez al año) que lo concientice sobre problemas de seguridad de la información.

Los usuarios deben recibir capacitación periódica (1 vez al año) que los concientice a una cultura de seguridad de la información.

Deben existir métodos que permitan afianzar la cultura de seguridad en el personal como:

- Correos electrónicos.
- Promover videos institucionales.
- Promover pláticas de seguridad.

2.11. Implementación

A fin de implementar controles de seguridad informática que sean efectivos y eficaces, la política de la Contraloría Municipal es:

a) implementar un conjunto coherente y equilibrado de controles de prevención, detección y recuperación;
b) implementar controles complementarios, y que se refuercen mutuamente, en todos los sistemas y actividades interrelacionadas. Debe evitarse el depender en un solo nivel de controles;

3. RESPONSABILIDADES DEL ÁREA DE SEGURIDAD INFORMÁTICA

3.1. Principios Generales

Todos los directivos y el personal tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de TI bajo su control, de acuerdo con las instrucciones y la capacitación recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y deben discriminarse dichas responsabilidades de aquéllas que sean incompatibles cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

3.2. Responsabilidades

a) Desarrollar, revisar y actualizar las políticas y normas.
b) Acordar las prioridades de seguridad informática;
a) Dar asesoramiento sobre la seguridad en los Sistemas Informáticos;
b) Investigar los aspectos penales de las violaciones de la seguridad informática, cuando sea necesario.
c) Garantizar que la seguridad de todos los activos de Tecnologías de la Información esté debidamente protegida.

3.3. Personal

Todos los servidores públicos y personal que utilicen sistemas informáticos son responsables de:
a) cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;
b) mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;
c) proteger la seguridad de los equipos de cómputo, así como de la información bajo su control directo;
d) informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de la misma, incluyendo sospechas de divulgación de contraseñas.

4. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA.

4.1. Principios Generales

Los objetivos de la evaluación de riesgos son identificar y establecer las prioridades de los riesgos de Seguridad Informática y planear las acciones necesarias para reducir dichos riesgos a un nivel que sea aceptable para el H. Ayuntamiento. Por lo tanto, debe llevarse a cabo una evaluación de riesgos cuando éstos no sean claros o acordados, a fin de aclarar los requisitos de control y las prioridades de administración de Seguridad Informática:

a) daño potencial que pudiera surgir de una violación seria de la seguridad informática;
a) la probabilidad real de que ocurra dicha violación, teniendo en cuenta las amenazas imperantes y los controles complementarios individuales de los controles técnicos.

4.2. Evaluación de los Riesgos de Seguridad Informática

Se podrán aplicar las técnicas de gestión de riesgos a todos los sistemas informáticos o a los servicios o componentes individuales de los sistemas, cuando sea posible y conveniente.

El proceso de evaluación de riesgos debe considerar:

a) La importancia de la información, de los equipos, del software y de otros activos del sistema informático en cuestión;
b) El daño que pueda causarse como consecuencia de una violación seria de la seguridad de la información.

5. SEGURIDAD DEL PERSONAL.

5.1. Terminación de Contrato

Al momento de notificar la terminación del contrato de un empleado por cualquier motivo y en cualquier circunstancia, el H. Ayuntamiento debe considerar y cuando corresponda garantizar que:

1) Eliminar los derechos de acceso a los sistemas, cuentas de correo electrónico, acceso a Internet, aplicativos y demás oportunidades en las que pueda existir un uso no autorizado de los sistemas de Información.
2) Los servidores públicos y empleados del H. Ayuntamiento de San Felipe Tepatlán, Puebla y terceros contratados, deben de regresar los activos propiedad del Municipio utilizados durante su trabajo en el tiempo que duro su contrato.
   Los activos utilizados son:
   - Software
   - Hardware
   - Equipo de Oficina
   - Documentos
   - Información en medios electrónicos

6. SEGURIDAD FÍSICA

6.1. Principios Generales

Las instalaciones con fines específicos que alberguen equipos informáticos e información, requieren una mayor protección que la proporcionada a las oficinas comunes.

6.2. Principales riesgos en los Sistemas Informáticos

a) Inundaciones.

b) Riesgos potenciales en el suministro de energía eléctrica.
c) Incendios.

6.3 Protección contra Incendio y Explosión

Las medidas de prevención de incendios y explosiones deben incluir:

d) Probar con regularidad los sistemas de advertencia de incendios de acuerdo con la recomendación técnica especializada.
e) Capacitación adecuada en el uso de los equipos de extinción de incendios.
f) Eliminación de material inflamable, por ejemplo papeles y artículos de papelería de desecho.

6.4. Control Ambiental

La temperatura, la humedad y la ventilación dentro de las instalaciones que albergan equipos de computación y de comunicaciones y medios de almacenamiento de información debe cumplir con las normas técnicas estipuladas por los fabricantes de los equipos.

6.5. Suministros de Energía Eléctrica

Los suministros de energía eléctrica deben cumplir con las normas técnicas estipuladas por los fabricantes de los equipos.
Debe proporcionarse a los sistemas críticos una fuente alternativa de energía eléctrica adecuada, por ejemplo, generadores de reserva, y si fuera necesario, una fuente ininterrumpida de energía eléctrica (UPS).

6.6. Controles de Acceso Físico

Debe protegerse la seguridad física de las instalaciones y del personal de TI mediante los siguientes controles:

a) Los controles de acceso deben garantizar que solamente el personal autorizado pueda acceder a los Sistemas Informáticos.
b) Deben mantenerse en secreto las claves de acceso a los equipos de cómputo.

6.7. Visitantes

La definición de visitante incluye a todo empleado para el cual una oficina determinada no es su lugar habitual de trabajo. Los procedimientos aplicados para la recepción de todos los visitantes en las instalaciones u oficinas de Tecnologías de la Información deben:

a) estar centralizados en una sola área controlada;
b) siempre que sea posible, se debe recibirlos fuera del perímetro del área de seguridad.

6.8. POLÍTICAS DE SEGURIDAD FÍSICA

a) Política de Seguridad: Conjunto de reglas, leyes, criterios, y prácticas que regulan la forma de administrar, proteger y distribuir la información dentro y fuera del H. Ayuntamiento.
b) Seguridad Física: Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Sobre el resguardo de las zonas de trabajo

1. En caso de una emergencia (terremoto, incendio, etc.) deben ser usadas las puertas de emergencia.
2. Las oficinas deben permanecer cerradas con llave cuando no se encuentre el personal responsable del área.
3. Se prohíbe hacer uso indebido de los recursos informáticos o de comunicaciones tales como equipo de cómputo e impresoras.

6.9. Visitas de Personal de Soporte Técnico

Se requiere tomar medidas de prevención adicionales para el personal de soporte técnico de Tecnologías de la Información que visiten las instalaciones.

De ser necesario, deben hacerse copias de resguardo de la información antes que los ingenieros tengan acceso a los sistemas o los equipos.

Al finalizar el trabajo de soporte técnico, deben realizarse las verificaciones correspondientes, cuando sean necesarias, para confirmar que:

- Se haya finalizado con éxito el trabajo autorizado.
- No haya habido ningún acceso no autorizado a los sistemas.
- La información permanece en su mismo estado, o que se los restableció a su estado original anterior al trabajo efectuado.
- Las computadoras no tienen virus.
- Las contraseñas de acceso a los sistemas no se modificaron.
- No deben sacarse del H. Ayuntamiento los medios magnéticos que contengan información confidencial.

6.10. Equipos

Debe protegerse la seguridad de los equipos mediante las siguientes medidas generales:

a) Deben guardarse los equipos bajo llave y asegurarlos cuando sean dejados sin supervisión.
b) se debe ubicar los equipos de manera que se reduzca el acceso innecesario.
c) no deben ubicarse los monitores ni las impresoras cerca de las ventanas, ni colocarlos de forma tal que puedan ser fácilmente observados;
d) debe prohibirse el comer, beber y fumar.
e) los procedimientos deben garantizar que el mantenimiento de los equipos se lleve a cabo de acuerdo con las recomendaciones de los fabricantes;

6.11. Cables

Siempre que sea posible:

a) Las líneas eléctricas y de telecomunicaciones deben ingresar en las instalaciones de forma subterránea, con instalaciones alternativas disponibles desde otra fuente y a través de una ruta de ingreso independiente.
b) Los cables deben ser enrutados e instalados de manera que se evite cualquier interferencia o daños accidentales o deliberados.
c) Los cables instalados en locales compartidos no deben estar al alcance de los otros edificios.

6.12. Medios de Almacenamiento de Datos y Software

Deben protegerse los medios magnéticos mediante controles de seguridad física adecuados que incluyan el almacenamiento de la información o el software importante en gabinetes o cajas fuertes a prueba de fuego. Las instalaciones destinadas al almacenamiento de la información ubicadas en otros lugares deberán recibir el mismo nivel de protección física que aquéllas ubicadas dentro de las instalaciones.

6.13. Eliminación de Desechos y Otros Materiales

El material de desecho y los equipos excedentes de informática deben ser eliminados en forma segura. En particular:
La papelería membretada y los papeles que contengan información. No deben ser reciclados como hojas de borrador fuera de las instalaciones.
Debe borrarse toda información y software que permanezca aún en los equipos y dispositivos de almacenamiento de información, incluyendo las PC, los disquetes, CD- ROM y cintas magnéticas, antes que se deseche.

6.14. Política para el uso de contraseñas

Se debe proporcionar el correcto diseño y uso de nombres de usuario y contraseñas, así como establecer un estándar para la creación de contraseñas fuertes ó robustas, su resguardo y la frecuencia de cambio.

Todas las contraseñas de usuarios (email, web, desktop computer, sistemas, etc.), deberán ser cambiadas cada 2 meses.

2.1.1 Guías Generales

Las contraseñas NO deben tener las siguientes características:

- Tener menos de 8 caracteres
- Ser palabras de diccionarios comunes
- Ser palabras comunes como:
  - Nombre de familiares, mascotas, amigos, compañeros, etc..

- o Nombre de marcas, compañías, hardware, software.
- o Cumpleaños, y otra información personal como dirección o teléfono.
- o Cualquiera de las anteriores escribiéndolos al revés.
- o Cualquiera de las anteriores seguida de un numero como secreto1, 1secreto.

Las contraseñas robustas deberán seguir las siguientes características:

- Tener caracteres en mayúsculas y minúsculas
- Tener números y caracteres especiales .0-9, ¡@#$^&()+l~-=\´{}[]:";´<>?,./)
- Utilizar al menos 8 caracteres alfanuméricos
- NO utilizar información personal, nombre de familiares, etc.
- NO utilizar el usuario como contraseña.
- Las contraseñas NO deberán ser almacenadas medios electrónicos.
- Las contraseñas deben ser creadas de tal manera que se puedan recordar utilizando algún tipo de algoritmo relacionado.

2.1.2 Resguardo de contraseñas

No se deben compartir las contraseñas con ninguna persona, incluyendo asistentes o secretarias, todas las contraseñas deben ser tratadas como sensibles y confidenciales. Recomendaciones de resguardo:

- Nunca revelar la contraseña a través de una conversación telefónica.
- Nunca revelar una contraseña a través de un correo electrónico.
- Nunca hablar de una contraseña en frente de otras personas
- Nunca revelar la contraseña a compañeros de trabajo en vacaciones, cada quien debe tener su cuenta propia.

2.1.3 Bloqueos por exceso de intentos fallidos

En donde la tecnología lo permita, se deberá implementar un control que límite a 8 intentos de acceso fallidos, después de los cuales se procederá a bloquear la cuenta en cualquiera de las dos formas siguientes:

a) Por espacio de una hora con opción a restablecerla mediante la solicitud expresa al administrador, si la tecnología lo permite.
b) De manera indefinida hasta que si el titular de la cuenta de acceso solicite el restablecimiento mediante el procedimiento autorizado.

2.2 Responsables.

Todo el personal que utiliza sistemas informáticos, es responsable de cumplir con esta.

7. ADMINISTRACIÓN DE LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

7.1. Utilización de los Equipos y Sistemas

Los equipos y sistemas del H. Ayuntamiento de San Felipe Tepatlán, Puebla deben:

a) Utilizarse solamente para los fines autorizados.
b) Registrarse en inventarios actualizados.

7.2. Resguardo de la Información

Los procedimientos de resguardo deben:

a) Preparar la creación oportuna de copias de resguardo de toda la información y software que se requiera para respaldar las actividades esenciales y los planes de contingencia.
b) Garantizar que todas las copias de resguardo de información y software sean documentadas correctamente, y que sean probadas con regularidad para garantizar que se puede contar con ellas en caso de emergencia.
c) Ser integrados con los planes para garantizar la continuidad de las operaciones y los planes de contingencia de TI.
d) Enviar la información de resguardo con prontitud y de forma segura a un lugar de almacenamiento remoto seguro. Este lugar debe estar lo suficientemente apartado de las instalaciones primarias para que la posibilidad de que ambos se vean afectados por el mismo incidente al mismo tiempo sea remota.
e) Retener suficiente información de resguardo generada para los requerimientos básicos, legales y regulatorios.

7.3. Administración de la Capacidad

Deben planificarse y monitorearse los requerimientos de capacidad a fin de evitar fallas debidas a una capacidad inadecuada de los sistemas informáticos y de comunicaciones.

7.4. Registro de Fallas

Deben documentarse todas las fallas técnicas importantes detectadas en los sistemas informáticos y de comunicaciones.

Deben revisarse las medidas correctivas, a fin de asegurarse que no se hayan comprometido los controles de seguridad y que se autorizó debidamente la medida correctiva adoptada.

7.5. Procedimientos en Caso de Incidentes de Seguridad

Un incidente de seguridad es una falla en la confidencialidad, integridad o disponibilidad de la información que ha causado, o es probable que cause, algún daño material, financiero, de imagen o de cualquier otro tipo al H. Ayuntamiento de San Felipe Tepatlán, Puebla.

En caso de que se produzca una falla significativa en la seguridad informática, la Dirección debe:

a) Registrar y documentar todos los hechos pertinentes respecto a la falla de manera tal que puedan ser aceptados como evidencia legal.
b) Revisar y fortalecer a la brevedad los controles de seguridad informática a fin de evitar la recurrencia de la falla.

7.6. Controles Antivirus

Debe utilizarse un sistema estándar de detección de virus actualizado para:

- Escanear todos los archivos que ingresen en el entorno informático por e- mail, dispositivos USB o cualquier otra fuente externa tal como el Internet para identificar, informar y, si se considera necesario, eliminar virus informáticos en la primera oportunidad que se tenga.
- Escanear y, si fuera necesario, corregir o mantener en cuarentena todos los archivos enviados desde el H. Ayuntamiento a otras dependencias, proveedores y otras contrapartes externas por e-mail u otros medios para asegurarse de que el H. Ayuntamiento no esté distribuyendo virus sin saberlo.
- Actualizar las definiciones antivirus por lo menos una vez a la semana.
- Ejecutar por lo menos una vez a la semana el antivirus instalado en el equipo de cómputo.
- El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Las carpetas compartidas, dentro de una Red, deben tener una clave de acceso, la misma que deberá ser cambiada periódicamente.
- El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca parches de seguridad, atractivos premios o temas provocativos.
- Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
- No instalar productos que se descargan de Internet, ya que son una potencial vía de propagación de virus.
- Evitar ejecutar o abrir archivo con doble extensión.

- Si el antivirus detecta un archivo infectado que no puede ser reparado, entonces debe ser eliminado.
- Realizar respaldos de seguridad de la PC al menos una vez por mes.

Los ataques de virus significativo deben ser considerados incidentes de seguridad y tratados en consecuencia.

7.7. Conexiones de Internet

Por su estructura, la Internet es global y abierta. La DGSEI no puede confiar en la seguridad de la Internet y, por lo tanto, debe implementar un conjunto completo y autónomo de controles.

Para proteger la seguridad de la información que se transmite a través de la Internet. Esta norma aplica a cualquier servicio externo que sea prestado utilizando el protocolo de Internet (IP).
Todos las demás normas y principios de control aplican de igual manera para las aplicaciones de Internet, y en particular:

a) Está prohibida la navegación en sitios de contenido pornográfico, juegos, chats, ocio y todo aquellos que no sea justificable para el buen desempeño de las labores del Servidor Público.
b) no debe transmitirse información confidencial o referida a valores a través de la Internet sin antes aplicar controles adicionales (cifrado, por ejemplo).
c) Deben implementarse herramientas automatizadas para prevenir la recepción de códigos ejecutables provenientes de la Internet que pudieran representar una amenaza para la seguridad informática.

7.8. Transportación de la Información

Se deben implementar los controles apropiados para proteger a las partes involucradas contra fallas de seguridad durante la transportación de unidades de almacenamiento de información. Estos incluyen los requisitos para:

a) proteger la integridad del contenido de la información;
b) autenticar los puntos de origen y recepción;
c) proteger la confidencialidad de la información en tránsito;
d) registrar los detalles pertinentes en una pista de auditoria.

8. ADMINISTRACIÓN DE CAMBIOS Y PROBLEMAS

8.1. Principios Generales

El control inadecuado de cambios es una causa común de fallas en el sistema y la seguridad. Los procedimientos de administración deben ser documentados, lo cual abarca todos los tipos de cambios en los sistemas de producción, incluyendo software, equipos, maquinaria y servicios mayores.

9. PLANES DE CONTINGENCIA DE TECNOLOGIAS DE LA INFORMACION

9.1. Principios Generales

Deben existir planes de contingencia para minimizar la duración y el impacto en las operaciones de cualquier falla seria en la seguridad (es decir fallas en la confidencialidad, integridad y disponibilidad de la información). Como mínimo, los planes de contingencia deben estar preparados para recuperar los sistemas esenciales utilizando instalaciones alternativas en un periodo de tiempo aceptable si los sistemas principales se vuelven inaccesibles o inoperables.

SAN FELIPE
TEPATLÁN

Construir y Transformar