Lineamientos para la gestión de seguridad de la información, de la Administración Pública Municipal de Villa de Tezontepec, Estado de Hidalgo.

Palacio Municipal S/N, Col. Centro,
Villa de Tezontepec Hidalgo. C.P. 43880, México.
Tel: 743 741 0011 Ext. 126
secretaria_contraloria@villadetezontepec.org

OBJETIVO

Establecer las disposiciones en materia de seguridad de la información, a fin de preservar su confidencialidad, integridad y disponibilidad, mediante la administración de los riesgos tecnológicos, así como la gestión de incidentes a los que pueden estar expuestos los activos, bienes y servicios informáticos y de comunicaciones de la institución que procesan, almacenan, mantienen, protegen o controlan la información de la Administración Pública Municipal de Villa de Tezontepec, Estado de Hidalgo.

ALCANCES

El presente lineamiento es de aplicación general para el personal usuario de los activos, bienes y servicios informáticos y de comunicaciones de la Administración Publica Municipal de Villa de Tezontepec, Estado de Hidalgo, y de forma específica, para las personas servidoras públicas adscritas al Departamento de Tecnologías de la Información y Comunicación, conforme a su competencia en el diseño, implementación, administración y mantenimiento de los procesos de seguridad de la información y análisis de riesgos.

MARCO JURÍDICO

El presente lineamiento se encuentra alineado al marco jurídico y normativo siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado Libre y Soberano de Hidalgo
- Manual de Organización de la Administración Publica Municipal de Villa de Tezontepec, Estado de Hidalgo.
- Manual de Procedimientos de la Administración Publica Municipal de Villa de Tezontepec, Estado de Hidalgo.

Palacio Municipal S/N, Col. Centro,
Tel: 743 741 0011 Ext. 126

CAPITULO I
SEGURIDAD DE LA INFORMACIÓN

I.1 PREVENCIÓN

1) La seguridad de la información conlleva la implementación de medidas orientadas a su protección, indistintamente del formato, considerando como punto central la identificación y evaluación de los riesgos a los que está expuesta, así como la aplicación de los controles necesarios para mitigar la probabilidad de ocurrencia e impacto en caso de que se materialicen, de conformidad con el método que para tal efecto se utilice.

2) La seguridad de la información consiste en la preservación de los principios rectores de protección de la información siguientes, los cuales representan la base para el análisis y evaluación de los riesgos que pueden presentarse en los activos, bienes y servicios informáticos y de comunicaciones de la institución:

Confidencialidad, garantiza que la información sólo sea accesible para las personas autorizadas a tener acceso, siempre que cumplan los procedimientos establecidos para ello.

Integridad, salvaguarda la exactitud y la exhaustividad de la información y los métodos de tratamiento.

Disponibilidad, garantiza que las personas usuarias autorizadas tengan acceso a la información y a los activos, bienes y servicios informáticos y de comunicaciones de la institución, cuando sea necesario.

I.2 DETECCIÓN

Los riesgos en la seguridad de la información generalmente surgen por la presencia de amenazas a los activos, bienes y servicios informáticos y de comunicaciones de la Administración Publica Municipal de Vill de Tezontepec, Estado de Hidalgo, lo que da lugar a incidentes, entendidos estos como eventos no deseados, que pueden tener como resultado una pérdida, conforme a lo siguiente:

Pérdida de confidencialidad, cuando una o más personas tienen acceso no autorizado a información reservada a cierto personal usuario.

Palacio Municipal S/N, Col. Centro,
Villa de Tezontepec Hidalgo. C.P. 43880, México.
Tel: 743 741 0011 Ext. 126
secretaria_contraloria@villadetezontepec.org

Pérdida de integridad, cuando el contenido de la información se cambia, modifica o altera por personas no autorizadas, de manera que ya no es precisa, confiable o completa.

Pérdida de disponibilidad, cuando se pierde o daña el acceso a la información, de forma tal que no puede ser utilizada por las personas autorizadas cuando la requieran.

I. 3 RESPUESTA

Al determinar las amenazas o los riesgos a los que pueden estar expuestos los activos, bienes y servicios informáticos y de comunicaciones, también se identifica(n):

- Las personas responsables directas.
- Las vulnerabilidades a la infraestructura tecnológica.
- El grado de probabilidad de ocurrencia.
- El impacto de los riesgos en caso de materializarse.
- La afectación en los controles implementados.

Para la administración de riesgos es importante identificar los controles ya establecidos y, en su caso, determinar si es necesario modificarlos, eliminarlos o adicionar nuevos controles considerando su objetivo y los responsables de su implementación y seguimiento.

CAPITULO II
TIPOS DE SEGURIDAD DE LA INFORMACIÓN

II.1 SEGURIDAD DE REDES DE COMUNICACIÓN

1) Las redes seguras se centran en dos aspectos básicos, la autenticación y la autorización, por lo que las personas usuarias de la red deben demostrar su autenticidad y que están autorizadas para acceder a los datos específicos conforme a sus funciones y actividades.

2) La Administración Publica Municipal de Villa de Tezontepec, Estado de Hidalgo, por medio de la Jefatura de Tecnologías de la Información y Comunicación, es la responsable de

Palacio Municipal S/N, Col. Centro, Tel: 743 741 0011 Ext. 126

administrar los dispositivos de las redes de comunicación, para lo cual lleva a cabo las acciones siguientes:

- Implementar mecanismos para identificar las posibles fallas en la administración de redes de comunicación y eliminar las amenazas.
- Monitorear el rendimiento de las redes de comunicación para mantener en óptimo funcionamiento los servicios y aplicaciones que funcionan con *Internet*.
- Detectar, aislar y ejecutar soluciones a los problemas o fallas de las redes de comunicación, a fin de evitar afectaciones a las personas usuarias de datos, aplicaciones, dispositivos o sistemas conectados a la red.
- Administrar la configuración y el rendimiento de las redes de comunicación, mediante:
    i. El monitoreo de los dispositivos de las redes de comunicación.
    ii. La visualización de los patrones de tráfico de las redes de comunicación.
    iii. La gestión de cambios y configuración de las redes de comunicación.
    iv. El análisis y solución de los problemas en los enlaces y conexiones.

- Coordinar el aprovisionamiento de las redes de comunicación.

- Mantener los niveles de calidad de servicio en la administración de las redes de comunicación, a fin de garantizar el tráfico, confiabilidad y disponibilidad de la red.

II.2 SEGURIDAD OPERATIVA O DE DATOS

1) La seguridad de los datos comprende las medidas de protección empleadas contra accesos no autorizados preservando su confidencialidad, integridad y disponibilidad; en este contexto, se tiene implementado soluciones de seguridad y protección de datos tanto en el entorno local, como en la red, las cuales permiten detectar, evaluar y supervisar la actividad y amenazas a la información, bases de datos, programas de cómputo, bienes informáticos físicos y sistemas de información.

2) En materia de seguridad de datos, la Jefatura de Tecnologías de la Información y Comunicación, realiza las acciones siguientes con objeto de que los servicios de seguridad de la información preserven su confidencialidad, integridad y disponibilidad, así como para optimizar y priorizar su uso a fin de asegurar su correcta funcionalidad y brindar un nivel de seguridad que permita disminuir las amenazas a la infraestructura tecnológica:

- Realizar anualmente el análisis y evaluación de riesgos de seguridad de la información, a fin de identificar las amenazas y vulnerabilidades a las que pudiera ser

Palacio Municipal S/N, Col. Centro,
Villa de Tezontepec Hidalgo. C.P. 43880, México.
Tel: 743 741 0011 Ext. 126
secretaria_contraloria@villadetezontepec.org

susceptible, con el fin de administrar e implementar controles o planes de acción.

- Dirigir las acciones para administrar los riesgos, que conlleva su evaluación, tratamiento, aceptación y comunicación.
- Implementar o reforzar los controles de seguridad técnicos y organizativos para evitar pérdida de datos, filtraciones de información u otras operaciones de procesamiento de datos no autorizado.
- Establecer técnicas orientadas a reducir la exposición de datos reservados y confidenciales en las aplicaciones, tomando como referencia los principios establecidos en las disposiciones en materia de transparencia y protección de datos personales, así como los principios de seguridad de la información.
- Definir mecanismos de control para reforzar la seguridad existente, así como para reducir los riesgos a la seguridad de los datos e información las unidades administrativas, preservando su confidencialidad, integridad y disponibilidad, como son:

  i. Controles de evaluación
  ii. Controles descriptivos
  iii. Controles Operativos
  iv. Controles específicos de datos
  v. Controles específicos de usuarios

II.3 SEGURIDAD OPERATIVA O DE DATOS

1) El almacenamiento de archivos en la nube es un método que proporciona acceso compartido a los datos de los archivos, el cual permite crear, consultar, editar o eliminar los mismos en tiempo real y de forma simultánea desde cualquier ubicación con conexión de red. Las ediciones son visibles para las personas usuarias o grupos a medida que se realizan, y los cambios se sincronizan y guardan para visualizar la versión más reciente del archivo.

2) En materia de seguridad en la nube, la Jefatura de Tecnologías de la Información y comunicación puede realizar las acciones siguientes:

- Orientar a las unidades administrativas para determinar qué información puede migrar a la nube, como:

  i) Datos

ii) Funcionalidades o procesos

iii) Aplicaciones

iv) Servicios

- Supervisar los escenarios de servicios en la nube, a fin de presentar opciones de soluciones de almacenamiento con la capacidad, flexibilidad y rendimiento para cubrir las necesidades de la Administración Publica Municipal de Villa de Tezontepec, estado de Hidalgo.
- Coordinar con la persona proveedora o administradora del servicio, la operación, rendimiento, compatibilidad, disponibilidad y seguridad de la red.
- Orientar a las UA sobre las funciones o acciones que se pueden realizar con la información o datos en la red, la localización de contenidos y los controles o permisos que pueden establecer para restringir los accesos a personas usuarias no autorizadas, o bien, para limitar las acciones permitidas para la protección de datos.

II.4 SEGURIDAD ACCESO

La seguridad de acceso es un componente importante dentro de la arquitectura de seguridad, cuyo objetivo es detener los accesos no autorizados que han logrado eludir otras medidas de seguridad, por lo que se cuenta con mecanismos seguros que permiten autentificar a las personas usuarias para acceder a los sistemas de información, plataformas y servicios de red.

En este contexto la Jefatura de Tecnologías de la Información y Comunicación, tiene establecidos mecanismos de seguridad que requieren que las personas usuarias, ya sea dentro o fuera de la red de la ASF, estén autenticadas, autorizadas y validadas continuamente para el acceso a datos, sistemas y otros recursos para mantener la seguridad y prevenir amenazas digitales, conforme a lo siguiente:

- Regular el uso de la cuenta de correo electrónico asignada y de las contraseñas de acceso a la red y a los sistemas de información que se tengan habilitados para el desempeño de sus funciones, cuya seguridad depende de la privacidad con que las personas usuarias protejan su clave de acceso.
- Implementar mecanismos de control de seguridad para la autentificación de las personas usuarias y verificación de sus cuentas, con base en la experiencia sobre tecnologías

Palacio Municipal S/N, Col. Centro,
Villa de Tezontepec Hidalgo. C.P. 43880, México.
Tel: 743 741 0011 Ext. 126
secretaria_contraloria@villadetezontepec.org

del mercado y las mejores prácticas para la gestión de seguridad informática.

- Instrumentar medidas para salvaguardar la seguridad, confidencialidad, integridad y disponibilidad de la información y documentación, mediante la aplicación de claves de acceso, contraseñas, protección de lectura, escritura y ejecución de archivos, programas o sistemas.
- Supervisar la aplicación de los controles de administración asociados a los dispositivos de seguridad para autorizar el acceso y controlar los flujos de información desde y hacia las redes de comunicación institucionales.
- Realizar el monitoreo de contenidos *Web* para bloquear páginas que considere peligrosas, inadecuadas o maliciosas, a fin de identificar los riesgos a la seguridad de las personas usuarias.

II.5 SEGURIDAD DEL CENTRO DE PROCESAMIENTO DE DATOS

1) Los aspectos que destacan son la seguridad física y de la red, que considera la planificación de las instalaciones para evitar intrusiones físicas y, la implementación de programas y contraseñas de protección para evitar vulneraciones, cuya finalidad es garantizar que la información, aplicaciones y servicios de la institución contenidos en el centro de procesamiento de datos, estén seguros y protegidos.

2) En materia de seguridad del centro de procesamiento de datos, la Jefatura de Tecnologías de la Información y Comunicación, realiza las acciones siguientes:

- Supervisar la operación ininterrumpida del centro de procesamiento de datos, así como de los equipos y servicios de cómputo centrales.
- Coordinar la programación y ejecución de los servicios siguientes:
  1) Monitoreo a los servicios y sistemas informáticos, con envío de alertas en caso de presentarse cualquier incidente.
  2) Procedimiento de respaldo periódico y recuperación de la información en los servidores.
  3) Protección de las copias de seguridad o respaldo contra lectura, modificación y eliminación por personal no autorizado.
- Comunicar al Presidente Municipal cualquier incidente que se presente en el centro de procesamiento de datos, así como tomar las medidas necesarias para proteger y salvaguardar su seguridad ante cualquier eventualidad, dado que en este sitio se encuentran instalados los servidores, conmutadores, enrutadores, así como equipos de telecomunicaciones en los que se procesa y almacena información vinculada

con los procesos administrativos que se lleven a cabo.

- Coordinar la implementación, mantenimiento y ejecución de las siguientes medidas de seguridad física del centro de procesamiento de datos:
  1) Control de acceso mediante bitácoras de registro para el personal autorizado y el personal ajeno que por circunstancias extraordinarias deba ingresar.
  2) Protección de cableado eléctrico y de red con sistema de alimentación ininterrumpida.
  3) Prohibir el ingreso con líquidos o alimentos que puedan generar daño a la infraestructura.
  4) Restringir el acceso al centro de procesamiento de datos con equipos telefónicos, fotográficos, de audio o video.

- Implementar acciones que contrarresten el impacto operativo en caso de que un incidente afecte gravemente la infraestructura tecnológica.

CAPITULO III
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

III.1 ACCIONES

Con el propósito de minimizar los efectos de los incidentes de seguridad, la Jefatura de Tecnologías de la Información y Comunicación conforme al ámbito de su competencia, pueden ejecutar las acciones siguientes:

- Fomentar en las personas usuarias la cultura de seguridad informática y sensibilizarlas sobre la prevención, identificación de amenazas y vulnerabilidades, así como difundir, en su caso, las medidas para enfrentarlos.
- Recibir los incidentes reportados por las personas usuarias mediante la Mesa de Servicio.
- Realizar el análisis y categorización del incidente con el fin de determinar su causa, coordinando la evaluación de las vulnerabilidades y pruebas de penetración para detectar posibles fallas o debilidades de seguridad.
- Resolver y reanudar los servicios en operación normal en el menor tiempo posible, así como facilitar una recuperación rápida y eficiente de las actividades, minimizando la pérdida de información y la interrupción de los servicios.
- Realizar las acciones correspondientes para mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes.

Palacio Municipal S/N, Col. Centro,
Villa de Tezontepec Hidalgo. C.P. 43880, México.
Tel: 743 741 0011 Ext. 126
secretaria_contraloria@villadetezontepec.org

- Fungir como contacto central para recibir los informes de incidentes de seguridad, así como para difundir información esencial de estos.
- Documentar la gestión del incidente e integrar el reporte correspondiente para su presentación al Presidente Municipal.

III. 2 MESAS DE SERVICIO

Por medio de la mesa de servicio se reciben los reportes de soporte técnico o incidentes detectados por las personas usuarias.
Cuando sea necesario, la Jefatura de Tecnologías de la Información y Comunicación gestiona el apoyo técnico con la persona proveedora de los activos, bienes o servicios informáticos y de comunicaciones para resolver las solicitudes de reportes o incidentes, así como supervisar que se otorgue la atención según lo estipulado en el contrato

La atención y resolución del reporte o incidente en materia de seguridad se debe notificar a la Mesa de Servicio para que coordine con la persona usuaria o con su enlace administrativo el cierre de la solicitud o *ticket* en el sistema.

III. 3 RESPONSABILIDAD

El desconocimiento de estas disposiciones por parte de las personas usuarias no las exime de su cumplimiento.

El incumplimiento por parte de las personas usuarias a este documento, así como a la normativa en la materia, las hará acreedoras a las responsabilidades administrativas en que puedan incurrir y a las sanciones correspondientes.

Los presentes lineamientos fueron aprobados el 30 de enero de 2026 y entran en vigor al día siguiente de su publicación.

Elaboró	Revisó	Aprobó
Lic. Froylan Casasola Rodríguez Autoridad Substanciadora.	**Lic. Mario Enciso Pérez Titular del Órgano Interno de Control.**	**Lic. Miguel Moisés Gonzáles Bautista Presidente Municipal Constitucional de Villa de Tezontepec, Hidalgo.**

CIUDADANOS COMO TÚ AYUNTAMIENTO VILLA DE TEZONTEPEC 2024 - 2027 AUTORIDAD SUBSTANCIADORA

AYUNTAMIENTO VILLA DE TEZONTEPEC 2024 2027 CONTRALORÍA MUNICIPAL

CIUDADANOS COMO TÚ VILLA DE TEZONTEPEC 2024 - 2027 PRESIDENTE MUNICIPAL