LINEAMIENTOS PARA REGULAR LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS SENSIBLES DEL H. AYUNTAMIENTO DE AHUATLÁN

GESTIÓN 2024-2027

Ahuatlán
H. AYUNTAMIENTO 2024 2027
¡Un Gobierno para Todos!

ÍNDICE

ARTÍCULO 1

Los presentes lineamientos tienen como objeto establecer las bases que deberán observar las personas servidoras públicas adscritas al Honorable Ayuntamiento de Ahuatlán, Puebla., que constituyen un plan estándar de seguridad de la información y protección de datos sensibles.

ARTÍCULO 2

Para los efectos del Presente ordenamiento, se entenderá por:

- **Ayuntamiento:** Honorable Ayuntamiento de Ahuatlán, Puebla;
- **TICs:** Tecnologías de la Información y las Comunicaciones;
- **Derechos ARCO:** Acceso, Rectificación, Cancelación, Oposición de datos personales;
- **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Responsable:** Los sujetos obligados señalados en el artículo 1, párrafo 5, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Stakeholder:** Es un público de interés para una entidad gubernamental, empresa o asociación, que permite su completo funcionamiento, estos se relacionan con las actividades y decisiones tales como: empleados, proveedores, clientes, gobierno, entre otros;
- **On-premise:** Infraestructura en sitio en las instalaciones del cliente o en un centro de datos;
- **IaaS:** Infraestructura como Servicio;
- **PaaS:** Plataforma como Servicio;
- **SaaS:** Software como Servicio;
- **MFA:** Múltiples Factores de Autenticación;
- **SGSI:** Sistema de Gestión de Seguridad de la Información;
- **ISO 27001-ISO/IEC 27001:** Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por la International Organization for Standardization y por la International Electrotechnical Commission;
- **RGPD:** Reglamento General de Protección de Datos en la Unión Europea;
- **OWASP Top 10:** Open Web Application Security Project Top 10 sirve como referencia a los más comunes tipos de ataques a la seguridad informática;
- **Seguridad informática:** Área relacionada con la informática y la telemática que se enfoca en la protección de las plataformas virtuales de infraestructura y todo lo relacionado con la misma, y especialmente la información contenida como recursos circulantes a través de las redes de computadoras. También se refiere a la práctica de prevenir los ataques maliciosos, a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos, y

- **Seguridad de la información:** Métodos y procesos que procuran proteger los archivos de información en sus diferentes formas y estados.

ARTÍCULO 3

Las personas servidoras públicas adscritas al Ayuntamiento deberán considerar el uso de políticas y protocolos de seguridad para el ejercicio de las funciones, entendiéndose a estas por el almacenamiento, procesamiento, compartición y/o envío de información, con los niveles adecuados de seguridad según la clasificación del tipo de información.

ARTÍCULO 4

La información utilizada por las personas servidoras públicas se clasificarán en:

- Información Pública;
- Información Reservada, e
- Información Confidencial.

ARTÍCULO 5

La finalidad de estos lineamientos es minimizar los posibles riesgos, reducir las amenazas a la información y garantizar un correcto uso y/o tratamiento, así como asegurar el resguardo adecuado de los datos a proteger.

Con los presentes lineamientos se pretende limitar los impactos que pueda generar la posible pérdida de información importante y se busca garantizar que, en caso de un incidente, se esté en posibilidad de llevar a cabo una recuperación de la información.

ARTÍCULO 6

La seguridad de la información puede apreciarse como. un compendio de estrategias, políticas y/o mecanismos que garanticen las siguientes dimensiones de la información:

- **Confidencialidad:** Se refiere a las restricciones en el manejo de la información cuando conforme a la Ley General de Transparencia y Acceso a la Información Pública, así como la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla se establece que dicha información se debe clasificar como confidencial o reservada. Por lo tanto, el tratamiento de la información tendrá como finalidad la no divulgación y el apropiado resguardo de la información, considerando que solo deberán ser colectados los datos realmente necesarios a fin de salvaguardar la privacidad y adecuada imagen del propietario;

- **Integridad:** Se refiere a que la información se mantenga inalterada ante accidentes o intentos maliciosos, ya que sólo se podrá modificar la información mediante autorización, el objetivo de la integridad es prevenir modificaciones no autorizadas de la información;

- **Accesibilidad/ Disponibilidad:** Se refiere a que el sistema informático o plataforma de gestión de la información, se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos o desempeño, por ello es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados. Es de suma importancia prevenir interrupciones no autorizadas de los recursos informáticos;

- **No repudio:** Se refiere a que la información generada por un ente no puede ser negada, equivale a una firma manuscrita testificada en un documento en papel, y

- **Autenticación para garantizar privacidad de la información:** Se refiere a la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser, ejemplo, se puede considerar el caso de un usuario que se conecta a un sistema especificando un ID de usuario y una contraseña.

ARTÍCULO 7
El Ayuntamiento conforme a la disponibilidad es presupuestal y los recursos materiales, podrá optar por las siguientes soluciones de gestión informática:

- **Infraestructura en sitio (On-premise):** Generalmente infraestructura en centro de datos o instalaciones propiedad del dueño de la plataforma de gestión;

- **Infraestructura como Servicio (IaaS):** Se contrata a un proveedor en donde se brinda solamente la infraestructura física y virtual como un servicio;

- **Plataforma como Servicio:** Son generalmente ambientes virtualizados que ya cuentan con los servicios para alojar una plataforma de gestión documental, por ejemplo, los Servicios Web de Amazon, y

- **Software como Servicio:** Son soluciones usables tales como Zoom, Google Workspace, HubSpot o Microsoft Office 365.

ARTÍCULO 8
Los responsables de la seguridad constituyen a aquellas personas encargadas de la seguridad de la información en las unidades administrativas con las siguientes funciones:

- Elaborar y proponer las políticas de seguridad de la información;
- Detectar y proponer los riesgos y las posibles soluciones para mitigar las amenazas;
- Elaborar y proponer el marco normativo de seguridad y controlar su cumplimiento;
- Verificar la implementación de las políticas de seguridad y las actividades de control para mejorar la seguridad de la información;
- Liderar la implantación del SGSI;

- Supervisar la implementación de los controles y medidas técnicas y organizativas para asegurar los sistemas de información;
- Revisar periódicamente el estado de la seguridad de la información;
- Realizar el seguimiento de los incidentes de seguridad;
- Controlar y revisar los indicadores definidos;
- Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria;
- Revisarlos informes de auditoría;
- Gestionar roles y responsabilidades;
- Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de información;
- Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias, y
- Reportar al Comité de Tecnologías de la información de las cuestiones relevantes en materia de seguridad de la información.

Los Titulares de las unidades administrativas deberán asignar al responsable de la seguridad que tendrá las funciones antes descritas.

CAPÍTULO I DEL COMITÉ DE TECNOLÓGÍASDE LA INFORMACIÓN

ARTÍCULO 9

El Comité de Tecnologías de la Información será un órgano auxiliar del Ayuntamiento encargado de realizar las funciones siguientes:

- Coordinar la detección de los riesgos de los sistemas de información utilizados por las personas servidoras públicas;
- Proponer al Comité de Control Interno y Desempeño Institucional los riesgos identificados en la utilización de los sistemas informáticos;
- Proponer la solución de las cuestiones relevantes en materia de seguridad de la información, y
- Proponer al Ayuntamiento la normatividad municipal correspondiente.

ARTÍCULO 10

El Comité de Tecnologías de la Información deberá celebrar por lo menos 3 sesiones ordinarias durante el ejercicio fiscal.

ARTÍCULO 11

Las sesiones serán públicas y podrán concurrir a las mismas cualquier persona sin distinción alguna, sin embargo, se les solicitará guardar compostura y abstenerse de hacer manifestaciones ruidosas u ofensivas. En cualquier cosa que afecte el desarrollo armonizo de las sesiones, el Presidente del Comité solicitará guardar el orden, pudiendo, en su caso, ordenar el desalojo e incluso hacer arrestar a quien o quienes, por su comportamiento, vulneren el orden y paz del desarrollo de la sesión.

Si se estima necesario, la o el Presidente del Comité puede ordenar la suspensión temporal de la sesión, en tanto se procede a desalojar de la sala a quienes perturban la estabilidad, paz y tranquilidad de la sesión, pudiéndose declarar que se continúe como una sesión privada.

ARTÍCULO 12

Las actas de Sesión del Comité deberán ser actas circunstanciadas en la que contendrá como mínimo:

- Fecha y hora del inicio de la sesión;
- El lugar de la celebración de la sesión;
- Pase de lista;
- El orden del día;
- Los asistentes a la sesión, haciendo la declaración de que existe el quorum legal;
- Descripción sucinta de la discusión sobre cada uno de los asuntos del orden del día;
- Las consideraciones de cada uno de los asuntos contemplados en la orden del día;
- La votación de cada uno de los asuntos contemplado en la orden del día, indicando el número de identificación del punto de acuerdo;
- Fecha y hora de la conclusión de la sesión, y
- Nombre y firma de los asistentes a la sesión.

ARTÍCULO 13

Al inicio de cada sesión del Comité se deberá verificar el quórum legal, si no existiera el número suficiente para la declaración, se esperará a los ausentes hasta por treinta minutos; sin embargo, concluido el plazo no se reúne el mismo, se citará a una nueva sesión, previo el acuerdo de los asistentes.

ARTÍCULO 14

Una vez determinado el quórum legal, se deberá presentar, discutir y aprobar el orden del día, así la presentación, discusión y votación de los acuerdos del Comité se sujetará a dicho orden.

Durante el desahogo de la orden del día, cualquier miembro del Comité puede solicitar autorización para utilizar equipo de sonido, fotográfico o electrónico o de ayuda audiovisual para ilustrar a la asamblea; de igual forma puede solicitar traducción a algún dialecto o lengua de uso común en el municipio de que se trate, si fuera procedente en las asambleas públicas.

Los integrantes del Comité contarán con un máximo de quince minutos para realizar su intervención en las deliberaciones y discusión de los asuntos.

Los asistentes o invitados podrán hacer uso de la palabra, previo permiso del Presidente del Comité, quienes contarán con cinco minutos para su manifestación, pudiéndose prolongar

por los cuestionamientos de los integrantes del Comité, sin que pueda exceder sede veinte minutos.

ARTÍCULO 15
Los puntos de la orden del día ser aprobados o rechazados por mayoría simple o por unanimidad, sin embargo, aquel integrante del Comité podrá abstenerse de votar, debiendo manifestarlo expresamente y el Secretario Técnico deberá señalarlo en el acta de Sesión.

CAPÍTULO II SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 16
La implementación de cualquier sistema de Gestión de Seguridad de Información tiene aparejados los siguientes riesgos, los cuales son enunciativos más no limitativos:

Cambios del Presidente Municipal y los Titulares de las Unidades Administrativas;
Ampliación de los plazos de la ejecución del Plan de Implementación por no contar con los requisitos mínimos señalados en la norma ISO 27001;
Falta de compromiso de las personas servidoras públicas de la Institución respecto a la importancia de la seguridad de la información, y
Ampliación de los plazos en la presentación y aprobación de los documentos oficiales.

ARTÍCULO 17
El Comité deberá establecer las acciones de mitigación de los riesgos de la implementación de cualquier sistema de Gestión de Seguridad, como son, entre los cuales se encuentran de manera enunciativa más no limitativa:

- Dar continuidad a la ejecución de los planes aprobados;
- Establecer una política y objetivos de Seguridad de la Información estableciendo un compromiso para establecer los requisitos aplicables relacionados a la seguridad de la información;
- Validar el Sistema de Gestión de Seguridad de la Información a intervalos planificados para asegurar la conveniencia, mejora continua y efectividad;
- Contar con los conocimientos sobre la ISO 27001;
- Los miembros del Comité promuevan e impulsen los documentos emitidos en materia de seguridad de la información y las actividades de control;
- Hacer entrega de la información y documentación relacionada con la seguridad de la información a través de un plan de transferencia de conocimiento, y
- Los integrantes del Comité supervisen que todas las actividades sean realizadas dentro de los plazos definidos y solicitar a tiempo la intervención de los expertos técnicos.

ARTÍCULO 18
Para la implementación de SGSI se requiere lo siguiente:

- Instalación del Comité de Tecnologías de la Información;
- Capacitarse en temas como COBIT 5 FUNDATIONS, ISO27001, ISO3100 e ISO22301, así como en temas de seguridad de la información, ethical hacking y protección de datos personales;
- Realizar un Ethical Hacking en intervalos mínimos de tres meses para determinar las vulnerabilidades o intrusión a los sistemas informáticos, y
- Realizar una auditoría en materia informática especializada.

ARTÍCULO 19
La metodología recomendada para la implementación de un SGSI es PDCA (Plan-Do-Check-Act) conformada de la siguiente manera:

- **Planear (PLAN):** Reconocer una oportunidad y planificar el cambio;
- **Hacer (DO):** Probar el cambio;
- **Verificar (CHECK):** Revisar la prueba, analizar los resultados e identificar lo aprendido, y
- **Actuar (ACT):** Tomar acción basada en las lecciones aprendidas, si el cambio fue exitoso, incorporar lo aprendido, o, de lo contrario, intentar un plan diferente.

CAPÍTULO III MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN Y DATOS SENSIBLES

ARTÍCULO 20
Para el caso de las medidas de seguridad de la información de "Enfoque de Seguridad Online", cuando se utiliza un sistema de control de información dentro de un ambiente, con nube pública o privada, misma que tiene mayores peligros, por lo que se deben considerar algunos puntos a implementar y con mayor prioridad si se integran a algún tipo de red social o herramienta colaborativa tanto para los equipos desde donde se acceda como de en cualquier equipo que tenga conectividad a la red a donde pertenezca la plataforma, para lo cual se deberán considerar las siguientes medidas:

- Únicamente tener acceso a la plataforma a través de los bienes muebles autorizados por el Ayuntamiento;
- Los bienes muebles autorizados por el Ayuntamiento solo sean utilizados para las facultades y funciones correspondientes;
- Prohibido descargar sistemas informáticos no autorizados;

- Nunca aceptar solicitudes de amistad de desconocidos en redes sociales o herramientas colaborativas;
- Hacer el uso de contraseñas seguras en todas sus cuentas como son: una longitud de 16 caracteres de longitud; al menos una letra mayúscula; el uso de números no consecutivos; el uso de caracteres especiales como ¡"·$%&#/?; nunca utilizar las mismas contraseñas para todas sus aplicaciones; y, no utilizar información personal como direcciones, número de teléfono, número de cuentas bancarias, fechas de nacimiento, etc;
- Prohibido dar click en enlaces de sitios web no seguros;
- Tener desactivado el GPS o Google Maps de los navegadores, salvo el caso de las aplicaciones bancarias;
- Contar con software antivirus y antimalware en los equipos que cuenten con acceso a un sistema de gestión de información;
- Mantener actualizados los sistemas operativos y los últimos parches de seguridad. No guardar datos personales, usuarios o contraseñas en los navegadores; Deshabilitar cuentas viejas o en desuso;
- Prohibido utilizar los equipos dedicados a trabajo para permitir a personas no autorizados (tareas de recreación o tareas personales), y
- Nunca instalar software no autorizado por el Comité de Tecnologías de la Información.

ARTÍCULO 21.

Los mecanismos de protección física de componentes deben considerar cuatro mecanismos de protección que pueden ser:

- **Sistemas de alimentación ininterrumpida (SAI):** Equipos de protección de energía tipo UPS o plantas de respaldo que impidan un corte de energía a los equipos físicos;

- **Módulos de Seguridad de Hardware (HSM):** Dispositivos de hardware sólidos y resistentes a manipulaciones que aseguran los procesos criptográficos generando, protegiendo y administrando claves utilizadas para cifrar y descifrar datos y crear firmas y certificados digitales;

- **Firewalls físicos:** Dispositivos físicos similares a un servidor que filtra el tráfico dirigido a una computadora. Mientras que en modelos empresariales hace algunas décadas, el usuario conectaba un cable de red directamente a una computadora o servidor, ahora se conecta con un firewall de hardware y permite definir reglas sobre el tráfico de información, y

- **Gateways de Seguridad:** Dispositivos dirigen el tráfico a otras redes y crean vías de acceso seguras mediante perímetros de seguridad. Aseguran que se bloquee el tráfico no autorizado y combinan capacidades de seguridad cibernética adicionales, como la administración de contraseñas.

ARTÍCULO 22
Las medidas para controlar accesos y/o seguridad de las instalaciones se deben establecer las siguientes:

- Controles de acceso por RFID;
- Controles biométricos (huellas digitales, iris ocular, etc);
- Arcos de detección de metales;
- Aparatos de detección por rayos X (escaner);
- Cámaras de Monitoreo de Circuito Cerrado, y
- Bitácoras de auditoría de acceso.

Las medidas anteriores serán establecidas conforme a la suficiencia presupuestaria.

ARTÍCULO 23
El Comité de Tecnologías de la Información deberá contar con un Plan de Contingencia y de Recuperación de Desastres para garantizar el menor tiempo posible fuera de servicio.

ARTÍCULO 24
El Plan de Contingencia y de Recuperación de Desastres deberá contar:

- Contar con mecanismos de respaldo de la información: Implementar medios magnéticos o algún mecanismo de almacenamiento que permitan la recuperación de información;
- Eliminar puntos únicos de fallo en los componentes que soportan a la plataforma de gestión de información. Implementar componentes redundantes/resilientes o en alta disponibilidad;
- Implementar acciones de Recuperación de un Desastre (DR - Disaster Recovery). El uso de una plataforma secundaría (ya sea en un Sitio de Operación Alterno o una plataforma virtual en otra locación) y un Disaster Recovery Plan; que permita trasladar la carga a la plataforma secundaria y posteriormente que se haya resuelto la incidencia, permitir el regreso de la carga operativa a la plataforma primaria, y
- Contar con políticas de descargo de responsabilidad necesarios al realizar una recolección, resguardo y procesamiento de información (disclaimers) en apego a la Ley.

ARTÍCULO 25
Las medidas de seguridad de la información que se deben considerar la minimización de un posible riesgo de filtración de información son:

- **Restringir el acceso a información reservada y confidencial.** Esto se logra por medio de la implementación de controles de acceso a la información que van desde el uso de pruebas de confianza para la autorización de dichos usuarios, uso de contraseñas

seguras, cifrado de la información en los almacenamientos y el canal de transmisión, el uso de Multifactor de Autenticación (MFA - Multifactor Authentication, tales como el uso de tokens o aplicaciones de token dinámico o biométricos) y auditoría de transacciones dentro de las plataformas de gestión de la información. Todo esto generalmente debe ir en colaboración con medidas de seguridad física en las instalaciones que resguarden información física o digital;

- **Implementar políticas de confidencialidad**. Se logra por medio de la definición de una serie de instrucciones sobre cómo debe ser el manejo de la información por parte de los empleados/usuarios para garantizar la protección de datos personales o la propiedad de la información de la institución;

- **Mantener en constante actualización las estrategias y mecanismos de ciberseguridad.** Hacer uso de productos y servicios comerciales reconocidos en materia de seguridad informática, tales como herramientas de monitoreo, utilizar Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) tales como:
    - Registros de dispositivos perimetrales (Firewalls, IDS, Honeypots, VPN, etc);
    - Registros de eventos de Sistema Operativo (generalmente en servidores y en algunos casos en equipos de usuario);
    - Registros de endpoint (tales como dispositivos móviles o de escritorio);
    - Registros de aplicaciones;
    - Registros de proxy (servidor intermediario, generalmente para auditoría), y
    - Registros de loT (Internet de las Cosas).

- **Elaborar acuerdos de confidencialidad y no divulgación de información**. Todo empleado/usuario de una plataforma de gestión de la información debe estar de acuerdo y firmar sobre fa no divulgación de la información confidencial, restringida o sensible que pueda dañar a una persona o institución en cualquier forma. Por ello es de suma importancia que las partes involucradas no den a conocer datos a los que tienen acceso en el desempeño de sus funciones durante cualquier tipo de relación, ya sea laboral, comercial o de cualquier otra naturaleza, y

- **Implementación de políticas de retención de datos.** Es importante que la retención de la información sea siempre en apego a las instituciones que indiquen las normas de acuerdo con el tipo de información, ya que un empleado o usuario debe tener claro durante cuánto tiempo puede conservar dentro de una plataforma su información antes de considerarse una eliminación. Un estándar en la confidencialidad de datos y fa normativa propuesta por la Unión Europea y que sirve de marco de referencia en algunas instituciones de América, es el Reglamento General de Protección de Datos (RGPD).

CAPÍTULO IV DISPOSICIONES FINALES

ARTÍCULO 26.
La interpretación de los presentes Lineamientos corresponderá al Comité de Tecnologías de la Información.

AUTORIZACIÓN

Conforme a los artículos 169 fracciones IV y VII de la Ley Orgánica Municipal, se emite los siguientes Lineamientos para Regular la Seguridad de la Información y Protección de Datos Sensibles:

Número de registro	
MAP/LRSIPDS/01	
Fecha de Elaboración:	11 de diciembre de 2024
Fecha de aprobación por el Cabildo:	17 de diciembre de 2024
Elaboró y Autorizó	

Liliana Lezama Martiñón
Contralora Municipal del
H. Ayuntamiento de Ahuatlán, Puebla.

CONTRALORÍA MUNICIPAL AHUATLAN, PUE. 2024-2027