

**COMISIÓN DE AGUA Y
ALCANTARILLADO DEL MUNICIPIO
DE SAN SALVADOR HIDALGO**

**LINEAMIENTOS PARA LA
SEGURIDAD INFORMATICA**

**LINEAMIENTOS PARA LA SEGURIDAD
INFORMATICA**

Clave: LSI/CAAMSSH/2024

Fecha de Autorización: 14/02/2024

Núm. de Revisión: 1

CONTENIDO

Objetivo	1
Alcance	1
Definiciones	1
Capítulo I	3
Lineamientos para el Uso y Seguridad de los Sistemas de Información	3
De las Aplicaciones y Sistemas de Información	4
Obligaciones y Responsabilidades de los Usuarios	4
Atribuciones y Obligaciones de la Dirección	5
Capítulo II	5
Lineamientos Soporte Técnico, Mantenimiento Adquisiciones Tecnologías de la Información	5
De las Responsabilidades de los y las Usuarios	5
Capítulo III	6
La Adquisición o Contratación de Bienes y Servicios de Tecnologías de la Información	6
Autorización para la Adquisición de Equipo de Cómputo, Software y Telecomunicaciones	6
Validación para Adquirir Bienes y Servicios de Tecnologías de la Información	6
Características de la Solicitud de Validación	6
Requisitos para la Adquisición de Bienes y/o la Contratación de Servicios de Tecnologías de la Información	7
Prohibición de Emitir Validación Técnica de Bienes y/o Servicios de Tic ya Adquiridos	7
De las Sanciones	7

Objetivo

Establecer deposiciones administrativas y legales para la Seguridad y uso de los sistemas de información, así como mantenimiento, soporte y adquisiciones de las tecnologías de información de la Comisión de Agua y Alcantarillado del municipio de San Salvador, Hgo.

Alcance

Los presentes Lineamientos son de observancia obligatoria para todo los servidores públicos de la Comisión de Agua y Alcantarillado del municipio de San Salvador, Hgo.

Definiciones

Artículo 1. Para efectos se les presentes Lineamientos se deber entender por:

Antivirus. Software especializado deseado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la Red

Aplicación. Cualquier programa computacional de uso específico para la CAAMSSH que se encuentra en operación y que poetan desarrollarse de manera interna por servidores públicos especializados, por terceros de manera particular para el organismo a ser licenciadas por un varios proveedores contratados para tal efecto LA CAAMSSH Comisión de Agua y Alcantarillado del municipio de San Salvador, Hgo

Confidencialidad. Es aquella por medio de la cual se garantiza que determinada información está accesible únicamente a servidores públicos autorizados para tener acceso y es una de las piedras angulares de la seguridad informática; Correo Electrónico Servicio de la Red que permite a los usuarios enviar y recibe mensajes y archivos rápidamente también denominados mensajes electrónicos cartas electrónicas) mediante sistemas de comunicación electrónicos

Contraseña. Palabra clave mediante la cual el servidor público puede tener acceso a una aplicación, sistema de información o elementos de infraestructura básica.

Contraseña de administrador de equipo de computo Palabra clave que permite el acceso a un equipo de cómputo para configurarlo ampliamente. La configuración de los equipos de cómputo en el Ayuntamiento es responsabilidad de la dirección;

Data Center Centre de infraestructura en el que residen los sistemas de información, dependiente del Departamento de Administración de infraestructura, dependiente de la subdirección de infraestructura tecnológica perteneciente a la dirección.

Dependencia. Son las que integran la CAAMSSH

Equipo de Cómputo. Dispositivo electrónico de uso personal capaz de almacenar información, procesar datos y entregarle al servidor público los resultados de la información procesada. Equipo mediante el cual, en conjunto con el uso de la Red del Organismo se puede acceder a los Sistemas de Información;

Hardware. Conjunto de todas las partes tangibles de la Infraestructura. Sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos e incluye cables, gabinetes o cajas, de todo tipo y cualquier otro elemento físico involucrado. Es la contraparte complementaria del Software que es el soporte lógico en un elemento de Infraestructura;

Incidente. Cualquier anomalía del funcionamiento normal o baja desempeño de las aplicaciones o sistemas de información que requieren atención de la Dirección;

Infraestructura. Conjunto bienes informáticos, cableado, equipos de cómputo, equipos en el Data Center, de radiocomunicación, conmutadores telefónicos y otros equipos de naturaleza tecnológica, así como sus sistemas operativos, que funcionan como un sistema o como un conjunto de subsistemas, cuya operación y administración es competencia de la Dirección;

Internet. Conjunto de redes de equipos de cómputo y otros equipos físicamente unidos a través de medios alámbricos o inalámbricos que unen Redes o equipos en todo el mundo;

Lineamientos. Conjunto de reglas y normas para la seguridad informática, que son de observancia obligatoria establecidas en el presente documento.

Nodos. Es un punto de conexión, ya sea de Redistribución (un ruteador o un switch) o de destino (Equipos de Cómputo, Servidores) para la transmisión de datos. Aplica también para salidas disponibles en placas colocadas generalmente sobre la Red para conectar un cable de Red (Nodo de cableado estructurado);

Periféricos. Dispositivos de entrada y de salida que se conectan a un Equipo de Cómputo. Por ejemplo: escáner, impresora, teclado, entre otros;

Red. Conjunto operacional de toda la Infraestructura de transmisión de datos propiedad del Ayuntamiento incluyendo equipos, configuraciones, cableados, enlaces propios o subcontratados y políticas de uso;

Responsable del Servicio. Servidor público sobre quien recae la responsabilidad directa o delegada de un proveedor del Organismo;

Servidor Público. Los trabajadores que prestan un servicio físico, intelectual, técnico, o administrativo subordinado a la CAAMSSH

Servicios. Son todas las aplicaciones que están soportadas en la infraestructura para agilizar y automatizar las actividades del Departamento con el servidor público;

Seguridad Informática. Conjunto de controles y medidas necesarias cuya finalidad es garantizar la integridad, confidencialidad, acceso seguro y disponibilidad de la información institucional.

Servidor. Equipo de cómputo de altas prestaciones, compartida por múltiples usuarios y que puede albergar más de una aplicación o una aplicación que da servicio a varios usuarios;

Sistema Operativo. Programa o conjunto de programas computacionales que en un sistema informático (por ejemplo, un equipo de cómputo) gestiona los recursos de Hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes; **Sistema de Información.** Cualquier programa computacional asociado a una o más base de datos, de uso específico para la CAAMSSH que se encuentre en operación y que pueda haber sido desarrollado internamente por la Dirección, desarrollado y/o licenciado por uno o varios proveedores contratados para tal efecto; o bien, que esté bajo la administración de la Dirección. Los Sistemas de Información se encuentran instalados y configurados en la infraestructura de servidores pertenecientes al Data Center y sirve para soportar la operación interna general;

Soporte Técnico. Conjunto de actividades preventivas y correctivas orientadas a mantener en operación los Servicios de Tecnología de la Información (TI) dentro de rangos aceptables de rendimiento y que son desempeñadas por la Dirección;

Usuario. Servidor público que hace uso de al menos un servicio de TI;

Unidades Administrativas. Son las Direcciones, Subdirecciones, Departamentos, Coordinaciones Administrativas u homólogas que integran las estructuras orgánicas de las Dependencias;

Unidad de Informática. Unidad administrativa establecida en el organigrama de la dependencia o entidad que tiene como función principal atender los requerimientos de TI;

Virus Informático. Es un programa informático que se ejecuta en el Equipo de Cómputo sin previo aviso y que puede corromper el resto de los programas, directorios de datos e incluso el mismo Sistema Operativo.

Capítulo I

Lineamientos para el Uso y Seguridad de los Sistemas de Información

Para hacer uso de los servicios de tecnologías de la información relacionados con sistema de información, el personal de la CAAMSSSH, deberá solicitarlo por escrito a la Dirección General.

Artículo 2. En el caso de que la solicitud oficial no indique con precisión la función de la persona para quien se solicitan los accesos, estos podrán ser limitados hasta en tanto no se reciban las indicaciones sobre los detalles de los accesos requeridos.

Artículo 3. La Dirección General autorizará el uso de los sistemas de información por persona, de manera que la autorización se acompañará de nombre del servidor público y contraseña, que será de uso personal e intransferible, salvo en los casos que el Departamento justifique ante la Dirección.

Artículo 4. El servidor público recibirá en sobre cerrado su nombre de usuario y contraseña acompañado de una responsiva sobre el uso de cada sistema de información que se le haya autorizado que deberá firmar.

Artículo 5. En los casos que el Departamento autorice el uso común de un nombre de usuario para ser utilizado por un grupo de personas, cada persona será responsable del cumplimiento de los presentes Lineamientos, en el tiempo que utilice el sistema de información.

Artículo 6. Los sistemas de información de la CAAMAH estarán diseñados para ser usados dentro de la Red institucional y cualquier acceso a los mismos, desde un lugar diferente al lugar de trabajo del usuario se encuentra totalmente prohibido, salvo que exista previa autorización del Titular de la Dirección, con excepción de los publicados vía web.

Artículo 7. Los sistemas de información o aplicaciones, una vez puestos en operación por primera vez al cabo de su desarrollo, sólo deberán utilizarse mediante equipos de cómputo propiedad de la CAAMSSSH

Artículo 8. Cada servidor público será responsable de la información que capture y de las consultas que realice en los sistemas de información a los que tiene acceso autorizado.

Artículo 9. Es responsabilidad de la CAAMSSSH supervisar la calidad de la captura de información de los servidores públicos que está bajo su responsabilidad, así como de supervisar el uso adecuado de la información que se llegue a consultar por medio de los sistemas de información.

Artículo 10. La baja de cuenta de usuarios deberá ser solicitada mediante oficio dirigido al Director General.

De las Aplicaciones y Sistemas de Información

Artículo 12. Los mantenimientos a sistemas de información que impliquen dejar sin servicio a los servidores públicos serán programados en fines de semana o por las noches con el fin de no afectar la operación CAAMSSH. **Artículo 13.** Los medios de almacenamiento como memorias USB, discos DVD, etc., deberán ser destruidos antes de ser desechados. De la misma manera, los equipos de cómputo antes de darse de baja por el procedimiento respectivo, deberán ser formateados a bajo nivel.

Artículo 14. La Dirección Administrativa deberá informar de manera inmediata a la Dirección General, sobre los incumplimientos detectados al respecto de los presentes Lineamientos en sus Dependencias.

Obligaciones y Responsabilidades de los Usuarios

Artículo 15. Los servidores públicos deberán encargarse de los siguientes procedimientos respecto a seguridad informática:

- I. Utilizar la infraestructura de comunicaciones asociada a su equipo de cómputo, para acceder solamente a equipos locales o remotos a los que tenga autorización por parte de la Dirección;
- II. Verificar que su equipo de cómputo tenga configurado el protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado a su información en caso de retiro temporal;
- III. Conectarse a la red cableada e inalámbrica únicamente con la autorización de los Departamentos;
- IV. Resguardar en un lugar seguro los medios electrónicos en que tenga respaldada su información laboral relacionada con los servicios al Ayuntamiento;
- V. Cambiar cada mes la contraseña asignada; siempre que los sistemas de información o aplicaciones lo permitan;
- VI. Hacer uso exclusivo de las contraseñas asignadas por la Dirección, para lo cual, el servidor público deberá evitar compartirla o divulgarla;
- VII. Los servidores públicos deberán contar con la autorización de la Dirección para conectarse a la Red de manera alámbrica o inalámbrica. La solicitud de la autorización deberá ser gestionada por un responsable del servicio;
- VIII. Tener presente cuál es la información clasificada sobre la que tiene control en el desempeño de sus funciones. La información que se tenga almacenada en documentos electrónicos, se debe proteger con contraseña y podrá ser enviada o entregada únicamente a sus superiores. Cada envío de esta información reservada debe quedar registrado por escrito en documento impreso o en correo electrónico;

Artículo 16.- Los servidores públicos deberán evitar realizar las siguientes acciones:

- I. Consequir a intentar conseguir los medios para acceder a sitios de Internet que no le son permitidos por la dirección.
- II. Acceder a sitios de internet de contenido malicioso o de gestión de descargas;
- III. Enviar cadenas por correo electrónico;
- IV. Enviar cadenas por correo electrónico;
- V. Alterar o dañar los identificadores de los equipos de cómputo y/o sus periféricos;
- VI. Alterar la configuración de red que les fue asignada al momento de la instalación del equipo;

- VII. Tener instalados programas de gestión de descarga los cuales al ejecutarse se constituyen amenazas a la seguridad informática pues facilitan una vía para accesos no autorizados a la Red, sistemas o información del Organismo;
- VIII. Tomar bebidas o ingerir alimentos en las áreas donde se encuentren instalados los equipos de cómputo y/o periféricos;
- IX. Instalar algún tipo de dispositivo (AP, Router, Switch) para replicar y comprometer la seguridad o estabilidad de la Red del H. Ayuntamiento, sin previa autorización o conocimiento de la Dirección.
- X. Habilitar o instalar servicios (DHCP, Servidores WWW, FTP) en alguna computadora para comprometer y/o replicar configuraciones de Red del Ayuntamiento, sin previa autorización o conocimiento de la Dirección.
- XI. El usuario no está habilitado para formatear o intervenir ningún equipo de cómputo, redes y telecomunicaciones de la CAAMSSH.
- XII. Contravenir los presentes Lineamientos.

Atribuciones y Obligaciones de la Dirección

- I. Instalar en los equipos de cómputo de la CAAMSSH antivirus, sistemas de control de accesos, sistemas de monitoreo de código malicioso; así como éstas y otras definiciones sean actualizadas frecuentemente;
- II. Administrar las contraseñas de administrador de todos los equipos de cómputo del Organismo;
- III. Modificar los procedimientos de acceso a los sistemas de información con la CAAMSSH finalidad de mejorar la seguridad informática;
- IV. Asegurar que los nodos de cableado estructurado que no estén en uso, no estén habilitados; o si lo están, tengan habilitados en los puertos de switch el acceso por medio de listas de acceso por dirección física de Red;
- V. Adquirir la infraestructura y/o sistemas para uso específico de seguridad informática más actual

Capítulo II

Lineamientos Soporte Técnico, Mantenimiento Adquisiciones Tecnologías de la Información

Artículo 17. Las solicitudes podrán requerirse mediante oficio, correo electrónico dependiendo de la naturaleza o urgencia del servicio.

Artículo 18. Recibida la solicitud para su atención y dependiendo de la naturaleza de la misma, la Dirección General, podrá requerir autorización del Departamento, para que con base a la disponibilidad de los recursos, de los criterios de racionalidad en el gasto o de su justificación se dé cumplimiento a la misma.

Artículo 19. El servicio que brindará será únicamente para los equipos que son propiedad de CAAMSSH

De las Responsabilidades de los y las Usuarios

Artículo 20. Los servidores públicos reportarán los incidentes presentados en los equipos tecnológicos, los cuales afecten sus actividades laborales.

Artículo 21. Los servidores públicos que realicen un reporte, deberán brindar toda la información requerida y atender todas sus indicaciones, a fin de colaborar en la determinación de un diagnóstico adecuado, el cual servirá para clasificar el incidente y resolverlo o en su defecto

Capítulo III

La Adquisición o Contratación de Bienes y Servicios de Tecnologías de la Información

Autorización para la Adquisición de Equipo de Cómputo, Software y Telecomunicaciones

Artículo 22. La adquisición de equipo de cómputo, «Software» y telecomunicaciones, se autorizará cuando se encuentre justificada y autorizada por la Dirección General aplicando en lo conducente lo previsto por Control de los Recursos Públicos para el Estado de Hidalgo.

Validación para Adquirir Bienes y Servicios de Tecnologías de la Información

Artículo 23. Toda adquisición o contratación de Bienes y Servicios de Tecnologías de la información, independientemente de la partida presupuestal de donde se tomarán los recursos, deberá contar previamente una solicitud de validación a la Dirección General; permitiendo dicha validación establecer la viabilidad operativa y funcional de la compra o en su caso, sugerir la configuración más adecuada a los requerimientos planteados por el Personal usuario.

La vigencia de la validación técnica será de ciento veinte días naturales a partir de su aprobación por el Área Administrativa.

Características de la Solicitud de Validación

Artículo 24. Las solicitudes de validación para la adquisición de Bienes y Servicios de Tecnologías de la información deberán ajustarse a lo siguiente;

- I. El usuario es responsable de verificar, que con las características mínimas solicitadas, este vigente en el mercado, el bien o servicio solicitado.
- II. El Área Administrativa podrá solicitar el estudio de mercado que utilizaron las áreas usuarias para obtener las características técnicas generales con las cuales cumplen varias marcas, mismas que utilizaron para generar la solicitud de validación técnica.
- III. Se anexa como referencia el siguiente ejemplo, en el cual se puede apreciar que no solo se deberá indicar que cumple la característica del equipo, es necesario poner el valor obtenido del datasheet del producto revisado, también se aclara que las características comparadas deben de estar en un rango cercano donde puedan competir las diferentes marcas y que sea el costo quien determine la marca adjudicada, dichas características deberán en apego a sus necesidades técnicas mínimas.
- IV. Cuando se pretenda adquirir un equipo con características diferentes a los paquetes de cómputo vigentes o se solicite un equipo con marca y modelo, se deberá justificar por qué los paquetes vigentes no les servirían.
- V. En caso de requerir cartas de proveedores, éstas deberán de solicitarse en el campo de observaciones de la solicitud de validación técnica y deberá estar incluida en las cotizaciones para los trámites administrativos correspondientes.
- VI. Sin excepción de usuario y área, no se permitirán pre validaciones, es decir, revisión de solicitudes antes de ser enviadas formalmente para revisión (firmadas por el Director Administrativo ni por correo electrónico u otro medio).
- VII. Cuando se solicite un incremento en capacidad de almacenamiento y/o procesamiento, se deberá proporcionar la evidencia que demuestre que la solución actual está al límite de su capacidad o presenta fallas. Podrán presentarse como evidencia impresiones de pantalla,

registros de uso y comportamiento, las cuales deberán de hacer referencia a los equipos que requieren crecimiento o sustitución.

Requisitos para la Adquisición de Bienes y/o la Contratación de Servicios de Tecnologías de la Información

Artículo 25. En la adquisición o contratación de Bienes y/o de Servicios de Tecnologías de la Información se observará lo siguiente:

- I. La adquisición por sustitución o equipamiento sólo procederá por causa justificada. El equipo sustituido deberá ser puesto a disposición de las Áreas Responsables para su revisión y dictamen de reutilización o, en su caso, para su trámite de baja, poniéndose a disposición de la Dirección General.
- II. No se autorizará la compra de Bienes usados o remanufacturados, ni la adquisición de equipos <<caja blanca>> o <<ensamble>>, salvo para organizaciones que los usen específicamente con objetivos didácticos en arquitectura de <<Hardware>>;
- III. Para toda adquisición de Bienes, se deberá tomar en consideración adherirse a las categorías del documento: (Especificaciones Técnicas mínimas para la Adquisición de Bienes y Servicios de Tecnologías de la Información y Telecomunicaciones).

Prohibición de Emitir Validación Técnica de Bienes y/o Servicios de Tic ya Adquiridos

Artículo 26. En ningún caso se emitirá una validación técnica de Bienes y/o Servicios de Tecnologías de la información ya adquiridos.

De las Sanciones

Artículo 27. La Dirección solicitará vía oficio a la Comisario, para que en el ámbito de su competencia, inicie los procedimientos y aplique las sanciones por responsabilidad administrativa, relativas a los alcances de los presentes Lineamientos.

Vigencia

Los presentes Lineamientos entrarán en vigor a partir del día siguiente de la aprobación de la Junta de Gobierno.