CAAMPAO

COMISIÓN DE AGUA Y ALCANTARILLADO DEL MUNICIPIO DE PROGRESO DE ALVARO OBREGÓN

CEAA
COMISION ESTAIAL DEL AGUA Y ALCANTARILLADO
DIRECCIÓN DE ORGANISMOS OPERADORES Y ATENCIÓN A USUARIOS

LINEAMIENTOS DE SEGURIDAD INFORMÁTICA.
2024

DIRECTORIO

INGENIERO. EFRAÍN GONZÁLEZ PÉREZ
DIRECTOR GENERAL

LICENCIADO EN CONTADURÍA ANAYELI SERRANO LOPEZ
ADMINISTRADORA GENERAL

INGENIERO ALDO DAVID PEREZ CEDILLO
ÁREA COMERCIAL

INGENIERO FELIPE BARRERA HERNÁNDEZ
ÁREA TÉCNICA Y OPERATIVA

Introducción

La creación del presente manual es con la intención de hacer un buen uso y cuidado tanto de la información como de los recursos tecnológicos y con ello minimizar riesgos asociados con acceso y uso de la información del sistema de forma no autorizada.

De igual manera se evaluará y cuantificará los activos a proteger y en base a ello seguir aplicando medidas de prevención y correctivas para minimizar riesgos.

Objetivo

Establecer una gestión adecuada de la información, sistemas informáticos y el uso responsable de los mismos, siguiendo las políticas, normas, procedimientos, reglas y prácticas establecidas.

Alcance

Este manual de lineamientos de seguridad de información tendrá un alcance y aplicación obligatoria a todos los servidores de la CAAMPAO, servidores externos y terceros que tengan acceso a la información de la institución.

Normatividad aplicable

Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades o tareas específicas a nombrar de los lineamientos de seguridad informática entre otros son

- Constitución Política de los Estados Unidos Mexicanos.
- Ley de Transparencia y Accesos a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Orgánica de Instituto de Hidalgo.

- Reglamento General de la Ley Orgánica del Instituto Tecnológico de Hidalgo.

LINEAMIENTOS

CAPÍTULO 1

DE LA SEGURIDAD INFORMÁTICA EN LA INSTITUCIÓN.

El presente documento de lineamientos de seguridad informática debe ser revisado anualmente por CAAMPAO, así mismo autorizado cuando sea necesario y todo cambio deber ser autorizado por la Junta de Gobierno.

Los términos y definiciones utilizadas en el manual son las siguientes:

- Usuario: Todo empleado o prestador de servicios autorizado que haga uso de los activos o de los servicios informáticos de la institución para el desempeño de sus funciones consulta o atención al servicio.

- Activo informático: Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desarrollo de sus funciones usuario, tales como equipos de cómputo, impresoras, video proyectos, teléfonos, equipos de telecomunicaciones, software, información entre otros.

- Equipo móvil: Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, Radios, entre otros.

- Medio de almacenamiento removible: Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, otras), cartuchos de respaldo, discos externos y otros.

- Base de datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

- Derecho de autor: Protección legal que cubre las actividades y trabajos de creación de productos de cualquier tipo que sean plasmados de forma tangible o material de conformidad con el marco aplicable en la materia. Las leyes de derecho de autor garantizan al creador el derecho exclusivo de reproducir, creación de derivados o hacer público su trabajo.

- Derechos de propiedad industrial: Protección legal destinada a proteger las invenciones individuales e industriales y que prohíben la copia, venta, reproducción o importación de determinado producto sin autorización explícita del dueño de los derechos de propiedad intelectual.

- Software institucional: Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

- Software libre: También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

- Cifrar: Técnicas bajo las cuales se transforma la información (de texto claro a texto secreto) y que solo puede ser accedida si se cuenta con las llaves o contraseñas.

- Web, www (World Wide Web): Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

CAPÍTULO 2

DEL BUEN USO DE LOS ACTIVOS INFORMÁTICOS

Los usuarios que tengan activo informático asignado de manera personal para uso de sus funciones, son los únicos responsables de utilización, así como también de la información contenida en los mismos por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

Toda movilización de activo informático dentro o fuera de las instalaciones es responsable del resguarde.

Todo personal y terceros son responsables del buen uso de los servicios informáticos alojados en las instalaciones, así como en la nube, asignados para realizar sus funciones administrativas.

CAPÍTULO 3

PARA EL RESGUARDO Y CONSULTA DE INFORMACIÓN

Los que tengan a su cargo la información debe contemplar en su proceso de respaldo de información, el resguardo histórico en los equipos de escritorio, móviles (laptops) y servidores utilizados en el soporte, mantenimiento y operación del aplicativo SPEI.

La información histórica debe estar disponible por lo menos 6 meses y contar con lo siguiente:

- Registro de creación y borrado de cuentas de administración.
- Restablecimiento de contraseñas e intentos por restablecerla.
- Accesos exitosos al sistema operativo.
- Intentos de accesos al sistema operativo.
- Creación de cuenta(s) de administración.
- Incorporación de cuenta(s) existentes al grupo de administración.
- Borrado de eventos de auditoría.
- Modificación de la política de auditoría.

La Dirección General, deberá implementar mecanismos de accesos y autenticación de seguros para la consulta y escritura, de la información generada por CAAMPAO.

Para los usuarios que requieren acceso de consulta a la información, debe ser otorgado por la persona quien tenga esa información a su cargo.

La Dirección General, realizara revisiones periódicas a los derechos de acceso otorgados a los usuarios.

CAPITULO 4

SECCIÓN DE CONTROL DE CAMBIOS.

- **Seguridad en la infraestructura tecnológica:** Todos los equipos y herramientas que se utilicen y apliquen deberán estar configurados y que cumplan con los protocolos de comunicación seguros.
- **Dirección de tecnología:** Establecerá los procedimientos de forma mensual para la gestión de parches de seguridad en equipos de escritorio, laptop y demás servidores utilizados en el soporte, mantenimientos y operación.
- **Gestión de usuarios y contraseñas:** Las contraseñas de las cuentas con altos privilegios de administración local deberán ser resguardadas por la gerencia de seguridad de la información, accesos a los puertos físicos de conexión y dispositivos periféricos.
- **Resguardo y consulta de información:** Se deberá contemplar un proceso de respaldo de información históricamente en los equipos de escritorio, así como los móviles autorizados y servidores en el soporte, mantenimiento, etc.

CAPITULO 5

GESTION DE INCIDENTES O RIESGOS

Contará con un procedimiento para detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica el cual compete

la identificación, contención, recolección y resguardo de evidencias de seguridad informática para su notificación. Como este organismo no cuenta con un departamento especializado en informática, el ayuntamiento otorgara apoyo mediante el área de informática para las siguientes gestiones:

La atención de fallas o problemas menores de los equipos informáticos, se hará por vía telefónica o correo electrónico (atención inmediata y una solución a la falla detectada en hardware y software). Para los casos en que se tuviese que solicitar servicios de reparación o cambios de partes en los equipos y/o actualizaciones en hardware o software, se solicitara por escrito a la Dirección General.

La unidad de informática atenderá las fallas o problemas de los equipos informáticos que estén o no con mantenimiento preventivo y correctivo, documentará la causa de la falla, emitirá un diagnóstico y dará las recomendaciones a los usuarios de las posibles soluciones para la rehabilitación o reparación de los equipos.

La atención de fallas o problemas podrá realizarse en el lugar de trabajo dependiendo del problema presentado y de la factibilidad para solucionarlo.

CAPÍTULO 6

CLASIFICACIÓN DE LA INFORMACIÓN

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

Los dueños de los activos de información deben responsabilizarse de las necesidades de la institución para clasificar, compartir y/o restringir información, así como del impacto asociado a estas necesidades.

Para la incorporación de activos de información al inventario, se debe asignar una clasificación de seguridad y debe ser proporcionada por el dueño del activo.

Todos los usuarios que hacen uso de la información clasificada como registrada o confidencial, evitaran que sea accedida por personas no autorizadas.

CAPITULO 7

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.

Se debe disponer de procedimientos para etiquetar y administrar la información de acuerdo con su clasificación.

CAPITULO 8

DEL INTERCAMBIO DE LA INFORMACIÓN

Toda persona que intercambie información reservada y/o confidencial con el personal de CAAMPAO o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Todo convenio de CAAMPAO con terceras personas, para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

CAPITULO 9

PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS)

Todo equipo de cómputo institucional debe contar con solución antivirus.

Todo usuario que identifique una anomalía en su equipo de cómputo deberá reportarla a la dirección general.

Se harán revisiones en base al cumplimiento de medidas de seguridad informática como antivirus y actualizaciones.

CAPITULO 10

PRESTACIÓN DE SERVICIOS DE TERCEROS

Debe exigirse al personal contratado para suministrar bienes o prestar servicios de informática que cumplan con las normas y políticas de seguridad informática correspondiente y demás disposición legal relacionada con el acceso a la información.

Todo servicio informático realizado por terceros deberá ser monitoreado y revisado por la persona responsable de la contratación.

CAPITULO 11

GESTIÓN DE USUARIOS Y CONTRASEÑAS

La Dirección técnica de servicios informáticos debe contemplar los lineamientos de las Directrices de Gestión de Cuentas de Usuario, para la configuración de los accesos a los equipos de escritorio o móviles (laptops) utilizados en la operación del aplicativo de CAAMPAO.

Donde se establecen los lineamientos para gestionar contraseñas de usuario, así como, sus características de conformación, los cuales deben considerar mínimo lo siguiente:

- Formación mínima de 8 caracteres para operadores y estaciones de trabajo.
- Que contengan mayúsculas, números y caracteres especiales.
- Periodicidad para cambiarlas por una diferente al menos cada 6 meses.
- Bloquear el equipo después de 3 intentos fallidos.

El aplicativo debe contar con un control de contraseña seguro y un mecanismo de historial, para garantizar la no reutilización de las mismas.

Para las contraseñas de las cuentas con altos privilegios de administración local y sistema de arranque, deben cumplir como mínimo:

- Formación de contraseña mínima de 8 caracteres de longitud.
- Al menos una letra mayúscula.
- Al menos una letra minúscula.
- Al menos un carácter numérico.

Toda persona que requiera acceso a servicios informáticos institucionales requerirá de cuentas de usuarios y contraseñas u otro medio de autenticación.

Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al encargado que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional.