CONCEJO MUNICIPAL DE VILLAVICENCIO

POLITICAS DE SEGURIDAD INFORMÁTICA

La seguridad informática tiene que ser un esfuerzo conjunto. Creemos que es importante que los usuarios de nuestra corporación tengan en cuenta que la protección digital es una prioridad.

Capacitación en seguridad informática
Todo servidor o funcionario nuevo en el Concejo Municipal de Villavicencio deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

Sanciones
Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta Corporación, o de que se le declare culpable de un delito informático.

Protección de la información y de los bienes informáticos

El usuario o funcionario deberán reportar de forma inmediata a la **oficina de Sistemas** cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
El usuario o funcionario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones del Concejo Municipal de Villavicencio, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
Los computadores de escritorio, portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones del Concejo Municipal de Villavicencio únicamente con la autorización de salida del área de recursos físicos, anexando el formato de salida del equipo debidamente firmado por el Secretario General o por el jefe de la oficina de sistemas.

Protección y ubicación de los equipos
Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de sistemas, en caso de requerir este servicio deberá solicitarlo.

La oficina de recursos físicos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la oficina de sistemas.
El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores del Concejo Municipal de Villavicencio.
Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.
Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
Se debe evitar colocar objetos encima del equipo de cómputo u obstruir las salidas de ventilación del monitor o de la CPU.
Se debe mantener el equipo de computo en un lugar limpio y sin humedad.
El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal del área de sistemas.
Cuando se requiera realizar múltiples cambios en los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación a la oficina de sistemas a través de un plan detallado.
Se prohíbe rigurosamente al usuario o funcionario distinto al personal de la oficina de sistemas abrir o destapar los equipos de cómputo.

Mantenimiento de equipos
Únicamente el personal autorizado por la oficina de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.
Los usuarios deberán asegurarse de respaldar en copias de seguridad o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

Pérdida de Equipo
Funcionario que tenga bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
El servidor o funcionario deberán dar aviso inmediato al área de sistemas y a la Administración de recursos físicos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

RECOMENDACIONES

Relacionadas con los equipos de computo

- ✓ **Actualizaciones regulares del sistema** operativo y del software instalado en el equipo, poner especial atención a las actualizaciones del navegador web, el sistema operativo como

Windows es propenso a fallos, riesgo que puede ser aprovechado por delincuentes informáticos, frecuentemente se liberan actualizaciones que solucionan dichos fallos.

Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, nos ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la **Oficina de sistemas** en: Antivirus, Outlook, office, Navegadores u otros programas.

- ✓ **Tener un antivirus** actualizado con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
  Estar pendiente de la fecha de caducidad de la licencia con el fin de renovarla inmediatamente tan pronto esta se cumpla.
  Es recomendable tener instalado en los equipos algún tipo de software anti-spyware, para evitar que se introduzcan en el equipo programas espías destinados a recopilar información confidencial sobre el usuario.

Para prevenir infecciones por virus informático, los usuarios del Concejo Municipal de Villavicencio no deben hacer uso de software que no haya sido proporcionado y validado por la **Oficina de sistemas.**

Los usuarios del Concejo Municipal de Villavicencio deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la **Oficina de sistemas.**

Todos los archivos de computadores que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la **Oficina de sistemas**.

El icono del antivirus McAffe debe permanecer siempre en color rojo, y para Antivirus Norton de color amarillo con chulo verde si usted observa dicho icono en otro color, favor avisar inmediatamente a la **Oficina de sistemas**, para que se haga la revisión correspondiente.

Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario del Concejo Municipal de Villavicencio, distinto al personal de la **Oficina de sistemas** deberá intentar erradicarlos de los computadores.

- ✓ **Instale un Firewall** o Cortafuegos con el fin de restringir accesos no autorizados de Internet.

Relacionados con la navegación en internet y la utilización del correo electrónico:

- ✓ **Navegue por páginas web seguras y de confianza.** Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:
  - Deben empezar por https:// en lugar de http.
  - En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

- ✓ **Utilice contraseñas seguras**, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

- **Sea cuidadoso al utilizar programas de acceso remoto.** A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la **seguridad de su sistema.**

- **Ponga especial atención en el tratamiento de su correo electrónico**, ya que este se ha convertido en una de las formas más utilizadas para introducir código malicioso, llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:
  - No abra mensajes de correo de remitentes desconocidos.
  - Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
  - No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos como hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Estas cadenas de e-mails se suelen crear con el objetivo de captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, phishing o todo tipo de spam.

- Utilice algún tipo de software Anti-Spam para proteger su cuenta de correo de mensajes no deseados.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

Uso de dispositivos extraíbles

Cada Jefe de Área o dependencia debe reportar a la **oficina de sistemas** el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado. Funcionario o usuario que tenga asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

La oficina de sistemas del Concejo Municipal de Villavicencio, velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

Daño del equipo

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

ADMINISTRACIÓN DE OPERACIONES EN EL CENTRO DE CÓMPUTO

Política: Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica del Concejo Municipal de Villavicencio. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como Internet.

Los usuarios y funcionarios del Concejo Municipal de Villavicencio que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus o software espía.

La oficina de sistemas en cabeza del Jefe de Sistemas, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.

Cuando un funcionario no autorizado o un visitante requiera ingresar al área donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmado y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de Secretaria General, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del área de sistemas.

El jefe de la oficina de sistemas deberá llevar un registro escrito de todas las visitas autorizadas al Centro de Cómputo restringido.

Todo equipo informático ingresado al Centro de Cómputo restringido deberá ser registrado en el libro de visitas.

Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
El Jefe de la oficina de sistemas deberá solicitar a la Presidencia los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

Uso de medios de almacenamiento
Los usuarios y funcionarios del Concejo Municipal de Villavicencio deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.
Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC´s) del Concejo Municipal de Villavicencio serán registradas y podrán ser objeto de auditoría.

Adquisición de software
Los usuarios y funcionarios que requieran la instalación de software que sea propiedad de Concejo Municipal de Villavicencio, deberán justificar su uso y solicitar su autorización por la oficina de sistemas con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.
Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Concejo Municipal de Villavicencio, que no esté autorizado por la oficina de Sistemas**.**
El control de manejo para las licencias y el inventario de los Medios, paquete de CD´s será responsabilidad de la Oficina Sistemas en cabeza del Jefe de Sistemas, o su delegado, en caso de ausencia.
El Grupo de Apoyo (Técnicos) de la Oficina de sistemas tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Corporación.
En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.
Deben mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados. Cualquier otra petición de software deberá ser tramitada a través de la Oficina de sistemas, utilizando el formato llamado.. . . . . **FORMATO DE SOLICITUD DE ADQUISICIÓN, REPARACIÓN, ACTUALIZACIÓN, MANTENIMIENTO O CAMBIO DE MATERIALES Y EQUIPOS**
el cual se puede descargar de la página WEB
(http://www.concejodevillavicencio.gov.co)
Finalmente se procede a actualizar el inventario de licencias de Software cuyo contrato tiene una vigencia anual. Y se almacenará en Archivos que puedan ser cerrados con llave.

Cada semestre la **Oficina de sistemas** en coordinación con la Secretaría General, Recursos Humanos y la presidencia ofrecerán capacitaciones al personal administrativo y contratistas en el manejo y uso de las Tecnologías de Informática y Computación (TIC's), para de esta manera convertir estos en herramientas efectivas de trabajo, y que apoyen el quehacer diario en el Interior de la Corporación. La capacitación de nuestro personal estimula en gran medida la utilización de los programas adquiridos legalmente, evitando la práctica indebida de utilizar software no autorizado y así evitar su proliferación.

Administración de la Red
Los usuarios de las áreas del Concejo Municipal de Villavicencio no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización de la Oficina de sistemas.

Seguridad para la Red
Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Oficina de sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del Concejo Municipal de Villavicencio, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Uso del Correo electrónico
Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Concejo Municipal de Villavicencio, a menos que cuente con la autorización de la Oficina d sistemas.
Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Concejo Municipal de Villavicencio. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

Controles para la Generación y Restauración de Copias de Respaldo (Backups)
Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:
Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.
Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.
Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.
Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.
Se utilizará el programa WINRAR en la opción añadir para comprimir el listado de archivos o carpetas a respaldar.

Las copias de seguridad o Backups se deben realizar al menos una vez a la semana y el ultimo día hábil del mes. Un funcionario de la Oficina de sistemas, revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

Oficina de Sistemas
Concejo Municipal de Villavicencio