Personeria
Municipal de Armenia
Construyendo ciudadanía y paz

personeriarmenia.gov.co

PLAN DE SEGURIDAD TIC

2018 v1

INTRODUCCION

La implementación de un plan de seguridad de las TICs, es un proceso técnico administrativo cada día más importante en cualquier tipo de empresa o entidad sea de índole público o privado. Este proceso debe abarcar a TODA la entidad, debe de ser aprobado y fuertemente apoyado desde la gerencia, ya que, sin ese apoyo las medidas que se tomen no tendrán el efecto necesario.

Cabe anotar que en cualquier entidad u organización la seguridad de la información es responsabilidad de todos los empleados.

Clasificación de la información

Debido a que en la Personería Municipal de Armenia se maneja información que se considera como pública y puede ser visualizada por cualquier persona, también existe información privada que solo puede ser vista por la persona o grupo de personas que trabajen con ella; debe hacerse una clasificación de esta información de acuerdo a su objetivo y así poder aplicar el correcto sentido, tomando en cuenta las siguientes características:

- *Información crítica: Es aquella que es indispensable para garantizar la continuidad operativa de la entidad.*
- *Información valiosa: Es aquella que es un activo y tiene valor por sí misma.*
- *Información sensitiva: Es aquella que debe ser conocida por las personas que la procesan y solo por ellas.*

Después de clasificar la información será mucho más fácil aplicar medidas de seguridad que preserven las siguientes características:

Confidencialidad: garantizar que la información sea accesible solo a las personas autorizadas.
Integridad: mantener exacta y total la información.
Disponibilidad: acceso a la información cada vez que la requieran.
Protección: asegurar la información tanto de amenazas de virus, como de copias ilegales.

Los riesgos a los que se ven expuestas las entidades, hacen necesaria la creación de directrices que orienten hacia un uso responsable de los recursos. Las políticas de seguridad son documentos que constituyen la base del entorno de seguridad

informática y deben definir las responsabilidades, los requisitos, las funciones, y las normas a seguir por todos los funcionarios de la entidad.

En la Personería Municipal de Armenia, se deben tener responsables de del desarrollo, implementación y gestión de la política, así como se debe crear una directiva de uso, que es un documento en el cual se informa lo que se puede y no se puede hacer con los equipos de cómputo.

Concientizar a los funcionarios públicos y contratistas sobre los posibles riesgos no solo en el uso del pc, si no en la pérdida de información por diferentes motivos.

A continuación, se relacionan algunas políticas de seguridad para su conocimiento, aprobación y demás fines:

a. No suministrar información de la entidad a entes externos sin previa autorización.

b. Asegurar a través de los recursos informáticos asignados, la integridad, confidencialidad, disponibilidad y confiablidad de la información que administran, especialmente cuando la información está protegida por reserva legal y/o clasificada como confidencial y/o crítica.

c. Descartar el uso de dispositivos de almacenamiento masivo como memorias USB, SD, MMC, Micro SD, External Drives, entre otros.

d. No Realizar el envío ni transporte de información en equipos electrónicos y/o tecnológicos que manejen sistemas de interconexión inalámbrica tales como: agendas digitales, tablets y/o Ipad, y smartphones. A menos que cuenten con la supervisión o la debida autorización del área de Sistemas,

e. Nunca realizar actividades que alteren, generen pérdidas o daños en el desempeño de los aplicativos y/o de la Información. Toda vez que se necesite asistencia técnica por alguna falla de los equipos deberá ser informado al área de sistemas.

f. No instalar software no licenciado, ya que aumenta el nivel del riesgo de adquirir virus, software espía, hurto o divulgación de la información e inconvenientes de índole legal (Derechos de Autor). Lo cual es verificado por entes de control al momento de realizar auditoria de sistemas.

g. Nunca utilizar la red de datos (WAN y/o LAN) de la Entidad para: obtener, almacenar y difundir en los equipos de cómputo, material pornográfico, música MP3, videos, películas, comerciales, cadenas de correo (estas cadenas de correo suelen

ser tomadas como spam por lo cual se podría realizar un bloqueo del servidor de correo).

h. De ningún modo realizar conexiones de equipos de cómputo personales a la red de datos (WAN y/o LAN), a menos que cuenten con la debida autorización y supervisión del área de Sistemas.

i. No desconectar, apagar, ni colocar objetos pesados sobre los dispositivos de red como: switches, tomas reguladas, canaletas, puntos de red, etc.

j. Abstenerse de conectar a la red eléctrica, equipos que no pertenezcan a la Entidad.

k. No retirar equipos de cómputo que pertenezcan a la personería municipal que contengan información de la misma, sin previa autorización

l. Apagar los equipos de cómputo cuando finalice el horario laboral y/o se retire del puesto de trabajo asignado, de lo contrario se incrementa el riesgo de pérdida y/o difusión de la información.

m. Se debe bloquear el Equipo de Cómputo siempre que el funcionario se retire del puesto de trabajo.

n. Es prohibido el uso de dispositivos (módems) personales para el acceso a Internet, ya que aumenta el nivel de inseguridad y vulnerabilidad de la información.

o. Conectar los equipos de cómputo siempre a la energía regulada y protegida con UPS (los ups deben ser apagadas para alargar su vida útil), para evitar daños en estos.

p. Requerir al área de sistemas y control interno la habilitación de los puertos USB, ya que su uso está restringido en los equipos de cómputo.

q. Restringir el ingreso de equipos de telefonía celular y/o equipos que cuenten con sistemas de grabación, almacenamiento de datos y/o imágenes a los lugares definidos como críticos por la información que se administra.

Cuentas y Contraseñas:

A los funcionarios públicos y/o contratistas que laboren en la Personería Municipal de Armenia, que se les asigne un equipo de cómputo, se les establecerá una cuenta de usuario y clave de acceso, de igual forma se le definirá un perfil de usuario de acuerdo a sus funciones para: adicionar, modificar, consultar y eliminar información.

 Definir el tipo de contraseñas en forma alfanumérica, mínimo de ocho (8) caracteres de longitud, que contengan mayúsculas y minúsculas (sin espacios).

 No utilizar la misma contraseña para diferentes Sistemas de Información o aplicativos. Por ejemplo, para el correo y la ventanilla única.

 Exhortar a no utilizar como contraseña: nombres, apellidos propios o de familiares, número del documento de identidad, fechas conocidas o fáciles de adquirir, etc. del usuario.

 Bloquear o apagar, según sea el caso, antes de retirase del sitio de trabajo, el equipo de cómputo asignado al usuario.

Correo Electrónico:

 Conservar actualizadas y depuradas todas las cuentas de correo electrónico con dominio @personeriarmeia.gov.co

 De ningún modo utilizar de forma inadecuada el correo electrónico asignado por la entidad para uso personal o para recibir, almacenar y/o difundir, material pornográfico, música MP3, videos, películas, comerciales, cadenas, etc.

 Eliminar el correo electrónico, en caso de recibir archivos y/o programas adjuntos y desconocer el remitente, lo anterior para evitar la contaminación de la información del equipo de cómputo; con virus, software espía, hurto o divulgación de la información.

Copias de Seguridad:

 Realizar el backup periódico de la información correspondiente del equipo asignado al usuario. En caso de traslado o retiro de los funcionarios públicos y/o contratistas el jefe de cada dependencia deberá informar con antelación la información que el funcionario tenía a su cargo.

 Solicitar soporte al área de sistemas para realizar el procedimiento, en los casos que requiera el usuario copias de seguridad adicionales.

Normas de seguridad de la información a nivel físico:

 Archivar la información contenida en documentos físicos en sitios seguros, que impidan la copia, consulta y/o eliminación de esta, por personal no autorizado o por humedad o excesivo calor.

Carrera 14 No.21-14. Teléfonos: (6) 741 34 74 - 744 32 83
E-Mail: comunicaciones@personeriarmenia.gov.co - info@personeriarmenia.gov.co

 De ningún modo destapar los equipos de cómputo por parte de los funcionarios públicos y/o contratistas

 Responsabilizar al usuario por la información contenida en los documentos físicos que administra, los cuales no pueden estar en sitios inseguros que impidan la copia, consulta y/o eliminación de esta, por personal no autorizado.

 Eliminar los documentos físicos, es obligación del usuario que los administra.

Recomendaciones Adicionales de Políticas de seguridad

1. Instalar y mantener actualizado el software antivirus. Debe disponer de protección antivirus en todos sus equipos de escritorio y portátiles.

2. Utilizar únicamente software legal.
3. Navegación Segura. Acceda únicamente a sitios de confianza, Borrar las cookies, los ficheros temporales y el historial de manera frecuente.

4. Proteger una Red WIFI. Para maximizar seguridad en la red Wifi es necesario usar la siguiente lista de consejos en conjunto. Ocultar el SSID Ocultar el SSID (identificador de redes inalámbricas) al exterior es una buena medida para evitar las intrusiones, aunque este dato puede descubrirse fácilmente, aunque este se presente oculto. Cambiar el nombre SSID Usar cifrado wpa2 y cambiar la contraseña periódicamente.

5. Mantener información a salvo mediante una periódica realización de copias de seguridad.

6. Utilice sistemas de alimentación ininterrumpida (SAI). UPS Para evitar que los equipos informáticos no se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los “micro-cortes” y picos de intensidad, que resultan imperceptibles, es recomendable el uso de **ups** en cada equipo de la entidad.

Nota: Este plan de seguridad está sujeto a cambios y adopción por parte de la alta gerencia de la entidad.

Carrera 14 No.21-14. Teléfonos: (6) 741 34 74 - 744 32 83
E-Mail: comunicaciones@personeriarmenia.gov.co - info@personeriarmenia.gov.co