La Entidad Asesora de Gestión Administrativa y Técnica -EAGAT a través de la Gerencia, establece como política que todo proceder institucional debe estar orientado a la transparencia y cumplir con los principios y valores que la rigen.

Con este propósito, se adoptan los siguientes compromisos para garantizar la confiabilidad de los procesos que desarrolla en cada una de sus áreas:

Objetivo:

Propender por el correcto uso de los recursos informáticos de la entidad, mediante el establecimiento de, lineamientos y supervisiones periódicas para su cumplimiento.

Para efectos del presente documento se entiende como equipo de cómputo: monitor, teclado, mouse y cpu y, dispositivos adicionales al resto de los componentes como pueden ser escaners, impresoras multifuncionales, video ba, etc.

1. El área de sistemas debe tener un registro de todos los equipos propiedad de la entidad.
2. Los equipos dados de baja deberán descargarse en el tiempo preciso del inventario, de igual manera deben registrarse los que ingresan por compra o por cambio de equipo, con el fin de mantener la información actualizada.
3. Los equipos que son reubicados temporal o definitivamente deben ser soportados por un documento que registre el movimiento del mismo, si es de forma definitiva, debe ser descargado del inventario del área a cargo con su debida justificación.
4. Todo equipo de cómputo que sea propiedad de la entidad debe ceñirse a las normas y procedimientos establecidos dentro de las Políticas de Seguridad de la Institución.
5. Toda Información contenida, procesada o generada en los equipos de cómputo es propiedad de la entidad. Los equipos de propiedad de los colaboradores de la entidad no serán revisados y reparados en el área de sistemas.
6. Debe existir además de la cuenta de usuario, una cuenta de administrador que servirá para los efectos de mantenimiento del equipo cuando así se requiera bajo una contraseña que así lo identifique.
7. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales, alimentación eléctrica, y acceso restringido de acuerdo con lo establecido por las políticas de Seguridad de la Institución.
8. Ningún equipo debe tener contraseña en el encendido (BIOS) a menos que la CONFIDENCIALIDAD de la información allí contenida así lo requiera, Todos los equipos de cómputo solo podrán tener instalado el Antivirus oficial adoptado por la entidad, donde el área de sistemas garantizará su actualización permanente.
9. Toda memoria USB que sea conectada al equipo debe ser previamente verificada por el antivirus adoptado por la entidad.

ASIGNACION Y USO DE LOS EQUIPOS

La solicitud de asignación de equipos se realiza por escrito por parte del encargado del área donde se requiere, dirigido al área administrativa y, deberá indicar el nombre completo del usuario, y las actividades para las cuales fue contratado a desarrollar en el equipo (para dimensionar el tipo de equipo de cómputo que se asignará). Así como el software a utilizar, con el fin de establecer la existencia de la licencia o justificar su compra de ser necesario.

Todos los equipos de cómputo deben ser protegidos con un protector de pantalla desbloqueable por contraseña, durante los momentos que el usuario no lo esté utilizando. El protector deberá activarse automáticamente a los 10 minutos de inactividad del equipo.

El equipo de cómputo debe estar conectado a un regulador de voltaje o sistema de energía ininterrumpible.

La protección física de los equipos corresponde a la persona a quien es asignado. En caso de requerir el movimiento del mismo, debe solicitarlo al área de sistemas.

El usuario será el responsable del software y hardware del equipo de cómputo, en el caso que dicho equipo sea compartido con otra persona, la responsabilidad será compartida.

El usuario no está autorizado a alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos. (instalación y/o modificación de hardware y/o software existente en el equipo de cómputo, sin la autorización escrita respectiva).

El usuario deberá cambiar periódicamente su clave de acceso de acuerdo al grado de seguridad que se requiera.

Es responsabilidad del usuario tomar todas las medidas necesarias para proteger la información de su propiedad, datos y/o software, por accesos desde Internet a su computadora o bien de una contaminación por eventuales virus que estén circulando por Internet, o ingresados a través de dispositivos de almacenamiento masivo por lo que la entidad, NO será responsable por daños causados por virus transmitidos a través de los antes mencionados.

En el caso de contar con software Freeware (libre de licencia) y que sea de utilidad para el usuario, deberá indicarlo por escrito al área de sistemas, indicando el o los equipo(s) donde se requiere instalar, además de justificar su uso.
En caso de presentar una falla física o lógica, ésta se debe notificar al área de sistemas.

En ningún caso el usuario intentará reparar el equipo, únicamente informará la posible falla. De ser requerido, el equipo se desplazará al área de sistemas para su revisión y/o reparación de acuerdo con el procedimiento establecido.

PROHIBICIONES

Tener cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.

Obstruir las rejillas de ventilación del equipo, ya que puede causar recalentamiento y daño al equipo.

Conectar otros aparatos eléctricos como cafeteras, radios, entre otros, en el mismo estabilizador o tomacorriente donde está instalado su equipo de cómputo.

Colocar aparatos o extensiones eléctricas encima del equipo, pueden causar interferencia magnética.

Realizar instalaciones de software o hardware y configuraciones adicionales a los equipos, sin autorización del área de sistemas.

RESPALDO DE INFORMACIÓN

Será responsabilidad del área de sistemas asignar a cada usuario interno carpetas de red privadas y/o compartidas para el almacenamiento y respaldo de su información.

Será responsabilidad del usuario interno almacenar la información que deseé respaldar en las carpetas que le hayan sido asignadas por el área de sistemas.

La copia se realizará automáticamente al servidor, con la periodicidad definida por el área de sistemas, siempre y cuando el usuario cumpla con las recomendaciones realizadas para tal fin. (tener la información en la carpeta indicada, tener el equipo encendido de acuerdo a la programación de la copia).

Todos los respaldos de información en medio físico deberán ser solicitados por el usuario de manera escrita al área de sistemas y de ser el caso avaladas por el jefe inmediato

La información contenida dentro de los equipos de cómputo está bajo la responsabilidad de los usuarios siendo esta propiedad de la entidad.

NOMBRAMIENTO Y DISTRIBUCIÓN DE ARCHIVOS

El límite de la longitud de una ruta y nombre de archivo puede tener máximo 255 (doscientos cincuenta y cinco) caracteres.

Este total de caracteres es considerado desde el inicio de la ruta que se crea al asignar un nombre de archivo (nombre del disco (drive) C: y todas las carpetas anidadas para llegar al archivo ejemplo: C:\Documents and Settings\Administrador\Mis documentos/TDR Actas/Acta01).

Cuanto más profundas sus carpetas se aniden, más larga será la ruta y menos caracteres quedarán disponibles para leer el archivo en mención. Por lo tanto, un nombre de archivo que supere este límite presentará dificultades para ser copiado
desde su lugar de origen (backup) e incluso para ser abierto.

1. Por lo anterior la entidad define como políticas para el nombramiento de carpetas y
2. archivos las siguientes:
3. Al momento de crear carpetas el nombre de la misma no debe superar los 18
4. caracteres.
5. Se permiten máximo 10 carpetas anidadas
6. Para nombrar archivos, la longitud máxima será de 40 caracteres
7. Al momento de definir el nombre de la carpeta o el archivo tenga en cuenta lo siguiente:
   - No utilice tildes ni la letra ñ, ni caracteres especiales

- Puede hacer uso de los espacios simples (NO doble espacio), letras y números.
- No es conveniente el uso de símbolos como: \ / : * ? " . _ ___ , ' ''< > ... ¡ [ ] ( ) | Estos símbolos generan conflictos al momento de realizar o tratar de recuperar una copia de seguridad.

PORTATILES EXTERNOS

Para los colaboradores que trabajan la información institucional en sus computadores personales se aplicarán las siguientes políticas:

1. Se deberá informar al área de sistemas el uso de equipos externos para la asignación de los permisos para la inercia de la red
2. La información contenida y procesada en los mismos relacionada con sus actividades laborales es propiedad exclusiva de la entidad.
3. Cada usuario es responsable de la información allí almacenada y de su copia de seguridad.
4. La entidad no es responsable de dichos equipos ni de la información personal que allí se almacene.

MEDIDAS CORRECTIVAS

Los problemas o conflictos relacionados con el uso de la plataforma tecnológica o los servicios de red, y que no se encuentren especificados en estas políticas deberán tratarse directamente con el área de sistemas.

Si se detectan archivos, MP3, WAV FILE, FOTOS FAMILIARES, O SOFTWARE NO LICENCIADO serán eliminados con previo aviso al usuario, y se notificará al encargado del área a fin de determinar los correctivos a que diera lugar.

Comuníquese y cúmplase

Bogotá 26 de abril de 2019

CÉSAR AUGUSTO CASTILLO TORRES MD.
GERENTE

EAGAT

Elaboró: Juan Pablo Astudillo Matiz Tecnólogo en Sistemas
Reviso: Ma Piedad Astudillo V. Asesor de Calidad y Planeación