La política descrita a continuación aplica a todos los empleados de Activos y Finanzas S.A – MicroActivos S.A.S – Buitrago & Asociados y demás personas que por alguna razón tenga acceso a la infraestructura tecnológica de la compañía.

Esta política también aplica a todos los recursos tecnológicos e informáticos con los que cuenta la compañía (infraestructura de la red de datos, bases de datos, software, servidores, portátiles, equipos de escritorio).

USUARIOS Y CONTRASEÑAS

A cada persona que trabaja en la compañía se le asignara un usuario y contraseña proporcionados por el área de tecnología para acceder a cada uno de los aplicativos (acceso a internet, computadores, correo, CRM, sapiens, intranet). Los usuarios y contraseñas son de carácter personal y no es permitido el uso compartido de las mismas.

Cuando la persona olvide o bloquee una contraseña debe notificarlo por medio de una solicitud (ticket) de soporte para que le sea proporcionada una nueva contraseña. Las claves proporcionadas por el área de tecnología son cambiadas por el usuario al mismo momento de ser entregadas siendo el usuario el único responsable por salvaguardar dicha contraseña. Las claves deben contener más de 8 caracteres entre mayúsculas, números, caracteres y minúsculas. Las contraseñas deben ser cambiadas en un periodo de 60 días.

MANEJO DE LA INFORMACION

Cada persona es responsable de salvaguardar su información a través del servidor de archivos para la administración de almacenamiento y recursos compartidos que se controla a través de permisos por usuarios por Active Directory de Windows.

Está prohibido que los usuarios tengan acceso a información que no corresponde con su cargo sin previa autorización escrita de su jefe inmediato.

Los usuarios no pueden proporcionar información a personal que no labore en Activos y Finanzas S.A – MicroActivos S.A.S – Buitrago & Asociados ni de la forma de acceder a los aplicativos e información de la compañía sin autorización escrita de su jefe inmediato.

El usuario puede solicitar la realización de una copias de seguridad (backup) de su información lo puede solicitar al área de tecnología quien guardara dicha información en los equipos servidores de la compañía. Información que se encuentre en servidores, portátiles y equipos de escritorio que no

corresponda a labores exclusivas de la compañía (música, fotos, video) será eliminada sin previa autorización.

USO DEL COMPUTADOR

Está prohibida la instalación de software diferente a los previamente instalados y configurados en servidores, portátiles y equipos de escritorio de la compañía por el área de tecnología y autorizados por el gerente general y la gerencia de tecnología.

El usuario no podrá realizar copia, distribución, transmisión o cualquier práctica no autorizada de software o licencias adquiridos por la compañía, así como la instalación de software de la compañía en equipos no autorizados o de terceros.

Activos y Finanzas S.A – MicroActivos S.A.S – Buitrago & Asociados se reserva el derecho de proteger su inversión en software realizando auditorias programadas y no programadas a los equipos de la compañía para prevenir la realización de copias no autorizadas de software así como la verificación de programas que se hayan instalado sin autorización. Las personas que se les encuentre realizando dichas prácticas quedaran sujetas a sanciones disciplinarias, ya que la duplicación no autorizada de software legal o de documentación es una violación a la ley.

Los puertos USB, unidades de CD/DVD, memorias micro sd están bloqueados en todos los computadores de los usuarios para solicitar permiso para utilizarlos debe pedir autorización escrita a su jefe inmediato y este a su vez informarlo al área de tecnología.

Los usuarios no podrán reubicar equipos de cómputo o de accesorios (cables, cargadores, switch, teléfonos) sin autorización del área de tecnología.

No dejar visibles claves para el acceso al equipo, correo, CRM, sapiens, tickets de soporte.

CONDUCTAS INAPROPIADAS EN EL USO DE COMPUTADORES

El sistema y los computadores de Activos y Finanzas S.A – MicroActivos S.A.S – Buitrago & Asociados son para uso exclusivo de las tareas propias de la compañía y cualquiera de las siguientes conductas será considerada inapropiada:

1. Instalación o desinstalación de programas, cambio de configuración de los equipos (fondo de pantalla, protector de pantalla, direcciones IP etc.).

2. Modificación de la configuración del sistema operativo y demás aplicaciones del software operativo del equipo.

3. Sacar el equipo de las instalaciones sin previa autorización.

4. Destapar o cambiar partes del portátil o equipo de escritorio.

5. Colocar objetos pesados en el portátil o tapar las áreas de ventilación de los portátiles o equipos de escritorio.

6. No ubicar cosas que deterioren los cables de conexión de los portátiles o equipos de mesa (Patch cord (red), cables VGA, cables de poder).

7. El usuario debe velar por cuidar el equipo y no ponerlo a riesgos como derrame de líquidos, ingerir alimentos, dejarlo conectado todo el día al cargador (solo aplica para portátiles), golpes, caídas, etc.

8. El usuario debe revisar el estado en el que se entrega el equipo y en el momento de entregarlo hacerlo en las mismas condiciones que se le asigno.

9. El usuario es el responsable de la información guardada en el equipo y la perdida por mala manipulación de dicha información es solo responsabilidad del usuario.

10. El usuario es responsable del uso y custodia del portátil o equipo de mesa y en caso de extravió o hurto tendrá que responder por el mismo y dar aviso inmediato al área de tecnología.

ESCRITORIO LIMPIO

Los usuarios deben tener el escritorio del portátil o equipo de mesa limpio de información confidencial, esto con el fin de proteger, conservar y mantener la confidencialidad de los datos y evitar que personal ajeno consulte rápidamente cualquier archivo que se encuentre en el escritorio del portátil.

BUENAS PRÁCTICAS

1. No se debe utilizar como contraseña el mismo nombre de usuario.
2. No utilizar contraseñas con datos relacionados con el usuario es decir nombres de hijo(a), esposo(a), etc.
3. No dejar predeterminados los usuarios y contraseñas en los aplicativos (correo, CRM, sapiens, etc.)

4. Poner en conocimiento al área de tecnología cualquier situación que pueda poner en riesgo la seguridad de la información.
5. Si cree que su clave fue conocida por un tercero comuníquese con el área de tecnología para realizar el cambio inmediato.

ACTIVIDADES PERSONALES

El uso de la red de la compañía será de uso exclusivo para la consultar, guardar y modificar información de uso exclusivo de la compañía.