

 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	<b>MEDIDAS PREVENTIVAS Y DE CONTROL DE SOFTWARE UDNET</b>	
	Macroproceso: Gestión de Recursos	
	Proceso: Gestión de los Sistemas de Información y las Telecomunicaciones	

## MEDIDAS PREVENTIVAS Y DE CONTROL PARA EVITAR EL USO FRAUDULENTO DE SOFTWARE EN LOS COMPUTADORES DE PROPIEDAD DE LA UNIVERSIDAD.

### Licenciamiento de software para equipos de cómputo.

- Las áreas de soporte de TI son las encargadas de verificar y controlar el licenciamiento de software instalado en los equipos de la universidad, mediante la configuración de usuarios y permisos que no permitan la instalación de software por parte de los usuarios.
- La Red de Datos verifica y gestiona el software de los equipos asignados a la administración central para labores administrativas (no de carácter académico) ubicadas en las sedes Edificio Administrativo, Publicaciones, Aduanilla de Paiba y Emisora de la Universidad Distrital.
- El control de los equipos de las oficinas y laboratorios que dependen de cada Facultad, lo realiza el personal de soporte contratado por cada decanatura.
- El control sobre los equipos de IDEXUD, ILUD los debe realizar cada una de estas Unidades, así como de los equipos pertenecientes a convenios.
- El área de soporte desinstala todo software sin licencia de los equipos de cómputo a los cuales les brinda soporte, y sin perjuicio de los posibles problemas de operación que se deriven del software desinstalado. Sin embargo, se debe notificar al jefe de dependencia, sobre la desinstalación del software sin licencia.
- Para el caso del software que esté instalado en los equipos de cómputo diferente a la suscripción de Campus Agreement y que esté debidamente licenciado, se solicitará por parte de la Red UDNET la licencia o los respaldos respectivos de la adquisición de las licencias. En el caso de software libre instalado en los equipos de cómputo a los cuales el área de soporte presta sus servicios, se verificará la naturaleza de dicho software, en dicho caso no se realizará desinstalación.

### Configuración de equipos de cómputo de las áreas administrativas.

Los equipos asignados a labores administrativas disponen de un disco duro al cual se le realizan dos particiones generando la partición C: y partición D:

En la partición C: se instala todo el software ya sea con licencia paga o software libre. A esta partición solo tiene acceso el usuario administrador del equipo (personal de soporte).

En la partición D: se redireccionan los usuarios configurados en el equipo, con el fin de garantizar el acceso por personal de soporte en caso de generarse problema sobre la partición C:

 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	<b>MEDIDAS PREVENTIVAS Y DE CONTROL DE SOFTWARE UDNET</b>	
	Macroproceso: Gestión de Recursos	
	Proceso: Gestión de los Sistemas de Información y las Telecomunicaciones	

Sobre la partición D: se guarda la información que trabaja el usuario.

- a) Pertenencia al dominio de la Universidad: El área de soporte registrará los equipos de cómputo en el dominio local de la universidad administrado por la Red UDNET, Configurando los permisos que sean necesarios para la instalación de actualizaciones de seguridad y antivirus desde los equipos servidores dispuestos para dicha labor.
- b) Restricción para usuarios: Se tiene restringida la instalación o desinstalación de software en los equipos. Esta labor es de exclusiva ejecución del personal de las áreas de soporte. De igual manera los usuarios no podrán en ningún caso resetear o cambiar la contraseña del administrador de los equipos. Para los equipos que administra UDNET, se configura clave de BIOS y bloqueo para inicio del equipo desde medios externos.
- c) Instalación de software en configuración básica: Sistema operativo, software de aplicación, utilitarios y antivirus. El software instalado por el personal de soporte de la Universidad debe ser licenciado bien sea por la suscripción a campus agreement, la adquisición de software especializado, solicitud de entes de control o por la compra individual de licencias de software.
- d) Todo equipo de usuario final previsto para utilizar con el sistema operativo Windows® debe ser adquirido desde su compra con la licencia OEM de sistema Windows®. El personal de soporte actualizará a la versión con la que se cuente en el contrato de Microsoft que sea estable en el momento de la configuración básica.

**Permisos y grupos generados desde dominio por el área de Plataformas de UDNET para la configuración de seguridad local en equipos de cómputo del usuario final.**

- a. Los grupos que deben configurarse para establecer los permisos en la partición principal o partición de sistema operativo son: grupo administradores, grupo usuario y grupo SYSTEM. Las cuentas predefinidas por el sistema operativo se deben eliminar.
- b. Los grupos que deben configurarse para establecer los permisos en las particiones secundarias o particiones de almacenamiento de archivos de usuario son: grupo administradores, grupo usuario. Las cuentas predefinidas por el sistema operativo se deben eliminar.
- c. Los permisos definidos por el sistema operativo que se deben habilitar para el grupo administradores en todas las particiones del disco duro son: control total, modificar, lectura y ejecución, mostrar el contenido de la carpeta, leer escribir.
- d. Los permisos que se deben habilitar para el grupo usuarios en todas las particiones del disco duro son: modificar, lectura y ejecución, mostrar el contenido de la carpeta, leer escribir.
- e. En archivos y carpetas compartidas desde el sistema de almacenamiento institucional SAN/NAS se debe agregar la cuenta o grupo de dominio que tendrá acceso al recurso compartido, los permisos respectivos y las cuentas habilitadas para tal fin deberán ser claramente establecido y solicitados por el jefe de la dependencia.
- f. Para las impresoras compartidas se dará acceso al grupo de la dependencia. Los permisos que se deben habilitar son: imprimir, administración de impresora, administración de documentos.

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	<b>MEDIDAS PREVENTIVAS Y DE CONTROL DE SOFTWARE UDNET</b>	
	Macroproceso: Gestión de Recursos	
	Proceso: Gestión de los Sistemas de Información y las Telecomunicaciones	

### Cuentas de administrador local.

Las cuentas de administrador local creadas en los equipos son:

- a. Cuenta “administrador”: Cuenta preconfigurada por el sistema operativo. Responsable de la clave: grupo de soporte.
- b. Cuenta de sede o facultad del grupo de soporte: esta cuenta se debe crear localmente y añadirla al grupo de administradores para no utilizar la cuenta de administrador local. Responsable de la clave: grupo de soporte

### Grupo usuarios y grupo administradores

En el grupo USUARIOS sólo debe estar registrada la cuenta de usuario final, bien sea de dominio o local, se deben eliminar las cuentas adicionales instaladas por el sistema una vez ingresado al Dominio. En el grupo administrador solo deben estar registradas las cuentas de:

- a. Administrador de dominio responsable de la clave: área de plataformas
- b. Grupo de soporte de dominio responsable de la clave: grupo de soporte
- c. Cuenta administradora local responsable de la clave: grupo de soporte
- d. Cuenta administrador local auxiliar responsable de la clave: grupo de soporte

### Estructura de los directorios de instalación de software y almacenamiento de archivos de usuarios.

#### Estructura de directorios y partición de discos duros:

- Se debe realizar la instalación de sistema operativo, software de aplicación, software especializado, antivirus y utilitarios como acrobat reader, winzip o winrar, navegadores, drivers, java, SiCapital entre otros; . en la partición C:\.
- Los documentos y archivos del usuario deben ser guardados por defecto en la carpeta D:\USUARIO, así mismo se debe direccionar para cada perfil de usuario, la carpeta “Mis documentos” a la carpeta usuario ubicada en el disco D:\

### Contraseñas de administrador.

Contraseñas de administrador: la contraseña de administrador sólo debe ser de conocimiento de las personas encargadas del área de soporte de cada sede o facultad. En cualquier caso, la contraseña debe reposar en sobre sellado en la jefatura del área de soporte correspondiente a cada sede o facultad.

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	<b>MEDIDAS PREVENTIVAS Y DE CONTROL DE SOFTWARE UDNET</b>	
	Macroproceso: Gestión de Recursos	
	Proceso: Gestión de los Sistemas de Información y las Telecomunicaciones	

item	Tipo de usuario	incluido en el grupo:	Permisos partición c:				Permisos partición D:					
			ver contenido de la partición	lectura	escritura	instalación	modificar	ver contenido de la partición	lectura	escritura	instalación	modificar
1	Usuario administrador local	Administradores	X	X	X	X	x	X	X	X	X	X
2	Usuario administrador de dominio	Administradores	X	X	X	X	x	X	X	X	X	X
3	Usuario administrador sede	Administradores	X	X	X	X	x	X	X	X	X	X
4	Usuario Local	Usuarios	X					X	X	X		X
5	Usuario de dominio	Usuarios	X					X	X	X		X

*Tabla 1. Resumen de usuarios sobre un equipo de usuario final*

#### NOTAS:

- ✓ Para equipos portátiles y/o equipos de usuario final como el caso de desarrolladores que por su uso deben contar con la clave de administrador local, se hace entrega dejando evidencia de la responsabilidad en formato que se anexa
- ✓ La solicitud debe ser realizada desde el correo de la dependencia, dicha solicitud debe ser aprobada por el jefe; igualmente el formato debe ser firmado por el usuario final, el jefe de la dependencia y el personal de soporte que atendió el caso.
- ✓ Las modificaciones al sistema operativo solo serán realizadas por el usuario con perfil de administrador.