Política de DIRECTV Group

Su trabajo y como trabajamos en conjunto

Uso de Recursos de la compañía

Junio de 2005

Contenido

USO DE RECURSOS DE LA COMPAÑIA

USO DE RECURSOS DE LA COMPAÑIA

Panorama General

Este documento de políticas define el uso adecuado de los recursos de la compañía. Las políticas aquí descritas aplican a todos los empleados del Grupo DIRECTV y sus subsidiarias, incluyendo DIRECTV y DIRECTV Latinoamérica. También aplican a los contratistas, socios de negocios, distribuidores, clientes y cualquier otra persona que tenga acceso a recursos que sean propiedad de la empresa o que la compañía haya emitido, operado o para los cuales haya otorgado licencias.

Política

El uso de los recursos de la empresa es principalmente para apoyar las metas de negocios y los objetivos de la compañía. La empresa apoya un ambiente que fomente el uso de equipo de comunicaciones, computadoras, información electrónica y otro equipo de oficina como herramientas esenciales para apoyar el negocio de la compañía.

Entre los recursos de la compañía se encuentran los equipos de comunicaciones que sean propiedad de la empresa o que la empresa haya proporcionado, como teléfonos, teléfonos celulares, maquinas de fax, correo de voz, correo electrónico, otros equipos de cómputo y de oficina como fotocopiadoras, impresoras, computadoras, laptops, acceso a Internet y acceso a redes internas.

Los dispositivos de comunicaciones, computadoras y otros recursos electrónicos y equipo de oficina son propiedad de la compañía y los empleados no deben tener expectativa de privacidad con respecto a la información o datos que creen, archiven, envíen o reciban por medio de estos sistemas. La compañía se reserva el derecho de monitorear el uso individual de cada empleado de dichos recursos para fines de mantenimiento, análisis y otros propósitos de la empresa, con o sin previo aviso a los usuarios.

Se permite a los usuarios hacer uso personal ocasional y razonable de los recursos de la empresa. Como ejemplo de uso razonable está el uso de duración y frecuencia razonable, el uso que no incluya temas o materiales cuestionables u obscenos, el uso que no esté en conflicto con las políticas de la empresa contra el acoso, la discriminación o el conflicto de intereses, y el uso que no apoye actividades de organizaciones religiosas, políticas o ajenas a la empresa a menos que la compañía lo haya autorizado previa y explícitamente.

Consulte la política sobre Protección de la Información para obtener más información sobre la protección y el uso adecuado de Información de la Compañía que se puede transmitir por medio de los recursos de la empresa.

Responsabilidades

Usuarios/Empleados

Para el uso de correo electrónico, acceso a Internet y acceso a la red interna, cada usuario es responsable de garantizar que estos recursos sean empleados para los propósitos de negocio adecuados y en forma que no comprometa la confidencialidad de información registrada, privada, delicada o secreta de la compañía y que no se viole la ley o las políticas impuestas por la empresa. Los usuarios no deben esperar tener privacía alguna; todas las comunicación es electrónicas hechas a través de los bienes de la compañía se considerarán propiedad de la empresa y podrán ser objeto de monitoreo por parte de la compañía.

Los usuarios no podrán compartir contraseñas para el uso de bienes de la empresa, proporcionar acceso a computadoras o correo electrónico a usuarios no autorizados, o accesar el buzón de correo electrónico de otro usuario sin autorización por escrito del usuario o del supervisor inmediato del usuario. Asimismo, los usuarios no deberán buscar o accesar recursos de la compañía que no estén autorizados para ello. Los usuarios no podrán publicar o divulgar ningún tipo de información de acceso.

Los usuarios no pueden usar recursos de la empresa para enviar cartas en cadena o mensajes profanos, ofensivos, insultantes o que alteren de alguna forma el ambiente de la compañía. Esto incluye mensajes que no sean consistentes con las políticas y posturas de Recursos Humanos con respecto al acoso o a la discriminación. Además, los usuarios no pueden facilitar acceso no autorizado a información de datos propiedad de la compañía, sin importar quién desee accesarla. Si se requiere acceso remoto, solo se podrán emplear los servicios de acceso remoto aprobados por la empresa.

Los usuarios no pueden usar recursos de la compañía para accesar a foros de chat en Internet a través de sistemas que no soporte la compañía.

Los usuarios pueden codificar su correo electrónico únicamente con software aprobado por el departamento de Sistemas de la empresa por medio de una forma o solicitud de

software y deben proporcionar las contraseñas de los documentos y/o objetos de datos codificados al momento de la aprobación por un miembro de la gerencia de alto nivel.

Si un usuario recibe una amenaza por correo electrónico de parte de un usuario interno o una persona externa a la compañía a través de los servicios de la compañía, el usuario debe guardar el mensaje y dar aviso al departamento de Seguridad de inmediato.

Los empleados que usen teléfonos celulares con capacidad de tomar y guardar fotografías, ya sean equipos de la compañía o personales, se comprometerán a no violar las políticas de la compañía, incluyendo aquellas sobre acoso y discriminación y deberán cumplir con cualquier aspecto de privacía y otras leyes.

El mal uso o abuso de cualquier recurso de cómputo proporcionado por la compañía deberá reportarse a la gerencia y al administrador de sistemas correspondiente de manera inmediata.

Administrador del sistema de correo electrónico (E-Mail)

Cuando se sospeche que un usuario de correo electrónico haya cometido alguna violación o realizado alguna actividad prohibida con relación a las políticas aquí descritas, el administrador de sistemas de correo electrónico da aviso a Recursos Humanos en caso de que el usuario sea un empleado y se avisa al gerente responsable en caso de tratarse de un trabajador temporal.

Recursos Humanos

Recursos Humanos contacta al supervisor indicado en los casos en que un usuario comete alguna violación, hace mal uso o abusa de los recursos de la empresa. Recursos Humanos, en conjunto con la gerencia, determinará la acción disciplinaria que se deba tomar, dependiendo de la naturaleza del mal uso o abuso.

Gerencia

Para correo electrónico, acceso a Internet o acceso a la red interna, el gerente responsable debe solicitar, por medio de Recursos Humanos, que el administrador de sistemas de correo electrónico revise los registros electrónicos de un usuario en caso de detectar o sospechar que haya incurrido en una violación o actividad prohibida.

En conjunto con Recursos Humanos, la gerencia decidirá la acción disciplinaria que habrá de tomarse cuando un usuario incurra en una violación, en mal uso o abuso de los recursos de la empresa. El gerente responsable debe avisar a la agencia de empleo correspondiente cuando se sospeche que algún trabajador temporal haya cometido una violación o actividad prohibida con relación a las políticas aquí mencionadas. La gerencia es responsable de hacer cumplir estas políticas.

Procedimientos

Monitoreo de comunicaciones electrónicas

El almacenamiento electrónico, incluyendo los buzones de correo electrónico de los usuarios, carpetas de red compartidas y discos duros de las computadoras de escritorio, se monitorean como parte de los procedimientos comunes del negocio. En ciertas situaciones, como en el caso de un citatorio, la compañía se puede ver obligada a accesar y dar a conocer mensajes que se hayan enviado por medio de su sistema de correo electrónico.

Virus de computadoras

Los virus computacionales representan una amenaza seria a la seguridad de los sistemas de cómputo, redes y telefonía de la empresa. Se espera que los usuarios tomen las debidas precauciones para evitar la introducción de virus en la infraestructura de tecnología. Cualquier material introducido al ambiente de cómputo de la compañía debe de pasar por un procedimiento de revisión para detectar virus antes de insertarlos a los sistemas de cómputo. Queda prohibido instalar software o hardware sin la aprobación adecuada del directivo del usuario y del gerente de TI.

Devolución de equipo propiedad de la compañía

Los empleados tienen la responsabilidad de devolver todos los equipos que les hubiese proporcionado la compañía, como teléfonos celulares y computadoras laptop, cuando ya no haya un motivo de negocios que justifique la necesidad de tener posesión de dichos equipos o al terminar el contrato de empleo del usuario con la compañía.

Anexo A: Tipos de archivos filtrados

Los siguientes tipos de archivos/extensiones de archivos pasan por un proceso de filtración en el perímetro de la red corporativa y no se permite que archivos de este tipo entren desde redes externas ni salgan de las redes de la compañía:

Tipo de extensión de archivos	
.ade	Extensión de proyecto de acceso de Microsoft (Microsoft Access Project extension)
.adp	Proyecto de acceso de Microsoft (Microsoft Access Project)
.app	Aplicación Generada por Foxpro (Foxpro Generated Application)
.bas	Módulo de Clase Visual Basic (Visual Basic Class Module)
.crt	Certificado de Seguridad (Security Certificate)
.csh	(Unix Shell Script)
.fxp	Archivo de Foxpro (Foxpro File)
.ins	(Internet Naming Service)
.mda	Programa agregado de acceso de Microsoft (Microsoft Access MDE Add-in Program)
.mdb	Base de datos de acceso de Microsoft (Microsoft Access Database)
.mde	Base de datos MDE de acceso de Microsoft (Microsoft Access MDE Database)
.mdt	Datos Agregados de acceso de Microsoft (Microsoft Access Add.in data)
.mdw	Información de grupo de trabajo de acceso de Microsoft (Microsoft Access Workgroup Information)
.mdz	Programa Wizard de Acceso de Microsoft (Microsoft Access Wizard Program)
.mst	(Visual Test Source Files)
.ops	Archivo de Foxpro (Foxpro File)
.pcd	(Photo CD Omage o Visual Test Script)
.prf	Información de Perfil de Outlook (Outlook Profile Information)
.prg	Archivo de Programa Foxpro (Foxpro Program File)
.dot	Plantilla de Microsoft Word (Microsoft Word Template)

Los siguientes tipos de archivos/extensiones de archivo pasan por un proceso de filtración interna y no se pueden enviar a cuentas de usuarios internas:

Tipo de extensión de archivos	
.bat	(Windows Batch File)
.cdf	(IE Channel File)

.cha	Chat de Internet (Internet Chat)
.chat	Chat de Internet (Internet Chat)
.chm	HTML Compilado (Compliled HTML)
.cil	(Potential Trojan)
.cmd	(Windows Command Script)
.com	Programa MS-DOS (MS-DOS Program)
.exe	Windows Ejecutable (Windows Executable)

Tipo de extensión de archivos

.hta	Programa HTML (HTML Program)
.html	Página web (Web Page)
.htw	Página web (Web Page)
.js	Javascript (Javascript)
.mht	Documento MHTML (MHTML Document)
.mhtml	Documento MHTML (MHTML Document)
.msi	(Windows Installer)
.msp	(Windows Installer Patch)
.pl	(Perl)
.reg	Archivo de registro (Registry File)
.sct	Componente Windows Script (Windows Script Component)
.sys	Archivo de sistema (System File)
.vbs	(Visual Basic Script)
.wsc	Componente Windows Script (Windows Script Component)
.wsf	Archivo Windows Script (Windows Script File)
.wsh	Archivo de propiedades de huésped de Windows Script (Windows Script Host Settings File)
.xml	Documento XML (XML Document)
.xsl	Archivo XML con soporte de script (XML File with script support)
.url	Atajo Internet (Internet Shortcut)
.asp & aspx	Página web (Web Page)
.cpl	Extensión de panel de Control (Control Panel Extension)
.htt	Página web (Web Page)
.inf	Información de setup (Setup Information)
.isp	Características predeterminadas de comunicaciones de Internet (Internet Communication Settings)
.jse	Javascript Codificado (Encoded Javascript)

.lnk	Atajo de Windows (Windows Shortcut)
.msp & .mspx	Página web (Web Page)
.pif	Archivo de Información de programa (ejecutable) (Program Information File)
.scf	(Windows Explorer Command)
.scr	Protector de pantalla (Screen Saver)
.shb	Atajo a un Documento (Shortcut into a Document)
.shs	(Shell Scrap Object)
.vb	Visual Basic Script (Visual Basic Script)
.vbe	Visual Basic Script Codificado (Encoded Visuel Basic Script)