GUÍA SOBRE SEGURIDAD Y DERECHOS DE PROPIEDAD INTELECTUAL PARA INSTITUCIONES ACADÉMICAS ©

IVF International Video Federation

MPA

ifpi representing the recording industry worldwide

PROMUSICAE Productores de Música de España

AIE ARTISTAS INTÉRPRETES O EJECUTANTES SOCIEDAD DE GESTIÓN

egeda

SGAE SOCIEDAD GENERAL DE AUTORES Y EDITORES

FAP FEDERACIÓN PARA LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

AGEDI ASOCIACIÓN DE GESTIÓN DE DERECHOS INTELECTUALES

La mayoría de las instituciones académicas ya han establecido medidas específicas para garantizar el respeto y el cumplimiento del derecho de propiedad intelectual en sus redes informáticas. Esta guía ofrece unas pautas simples y prácticas para ayudar a los responsables de las universidades a transmitir, aplicar y hacer cumplir estas medidas en beneficio de los titulares de derechos y de la comunidad académica.

CONTENIDO©

03 ¿CUÁLES SON LOS RIESGOS?
04 ¿CUÁNDO HAY QUE ESTAR ALERTA?
05 PAUTAS PARA RESPETAR LOS DERECHOS DE PROPIEDAD INTELECTUAL
06 MODELO DE MEMORANDO
07 MODELO DE CÓDIGO DE CONDUCTA

Para las instituciones académicas, las violaciones de los derechos de propiedad intelectual suponen un problema legal, ético y de seguridad.

¿CUÁLES SON LOS RIESGOS? ©

La Ley de Propiedad Intelectual prohíbe la copia y distribución de música y películas en Internet por medio de sistemas informáticos sin el permiso de los titulares de derechos. Como creadores de propiedad intelectual, las instituciones académicas también entenderán la importancia de salvaguardar el material protegido por derechos de propiedad intelectual. Además, su responsabilidad les hace igualmente idóneos para informar sobre este tema a los jóvenes.

Para las universidades, las infracciones contra los derechos de propiedad intelectual también afectan a la seguridad informática. Sin las precauciones adecuadas, sus sistemas pueden ser utilizados indebidamente por usuarios internos o piratas externos, haciendo que sus equipos informáticos se conviertan en sistemas de distribución ilegal del material protegido. Esto provoca la existencia de una serie de riesgos legales y de seguridad para las instituciones, su personal y sus estudiantes.

Esta guía tiene como objetivo contribuir a que las instituciones académicas garanticen que sus redes informáticas permanezcan limpias de material pirata, protegiéndose de los riesgos legales y de seguridad.

PROCESOS JUDICIALES POR VÍA CIVIL Y PENAL

Prácticamente todos los países tienen leyes que tipifican como ilícito civil y penal la copia ilegal, la distribución y la puesta a disposición en Internet de materiales de terceros sujetos a derechos sin el permiso de sus titulares. Dichos titulares han mostrado una preocupación especial por el robo del material protegido que se utiliza en las redes informáticas académicas y públicas, sobre todo habida cuenta de la velocidad y escala con que se disemina este tipo de contenido. La mayoría de los centros escolares establecen normas para promocionar un uso responsable de sus redes informáticas, advirtiendo contra las infracciones de los derechos de propiedad intelectual. Desgraciadamente, en la práctica estas medidas no se suelen aplicar, lo que puede ocasionar que se lleven a cabo acciones legales no sólo contra los estudiantes, sino contra las propias instituciones académicas cuyos sistemas alberguen bases de datos con materiales protegidos ilegítimos, al actuar como servidores de distribución o facilitar la copia ilegal o "el intercambio de archivos".

BRECHAS DE SEGURIDAD

Un sistema que alberga software P2P puede entrañar serios riesgos para sus datos, confidencialidad y seguridad informática. Las páginas web ilegales, entre las que hay foros, blogs, grupos de noticias y servicios de intercambio de ficheros sin licencia, son el origen de gran parte de la música, películas, software y otros materiales protegidos ilegales, además de una fuente importante de:

Virus

Los virus pueden estropear los equipos individuales, destruir los contenidos de ordenadores y servidores, comprometer la infraestructura de seguridad y extenderse a través de la red; es más probable que esto suceda cuando una institución permite a sus usuarios conectarse a esa red con sus propios ordenadores que normalmente no tienen establecida una protección antivirus eficaz.

Programas espía

El software para intercambio de ficheros a menudo instala programas espía y de publicidad que informan sobre el uso que se está haciendo de ese ordenador en concreto, envían publicidad u otros ficheros no solicitados que consumen memoria y cuya eliminación puede resultar difícil y peligrosa.

Brechas en los cortafuegos

Muchos de los sistemas de intercambio de ficheros P2P dan instrucciones a los usuarios para configurar el cortafuegos de modo que abran los puertos necesarios para conectar los sistemas P2P entre sí. De esta forma, los virus y "gusanos informáticos" también pueden eludir la protección de los cortafuegos.

Excesivo consumo de recursos

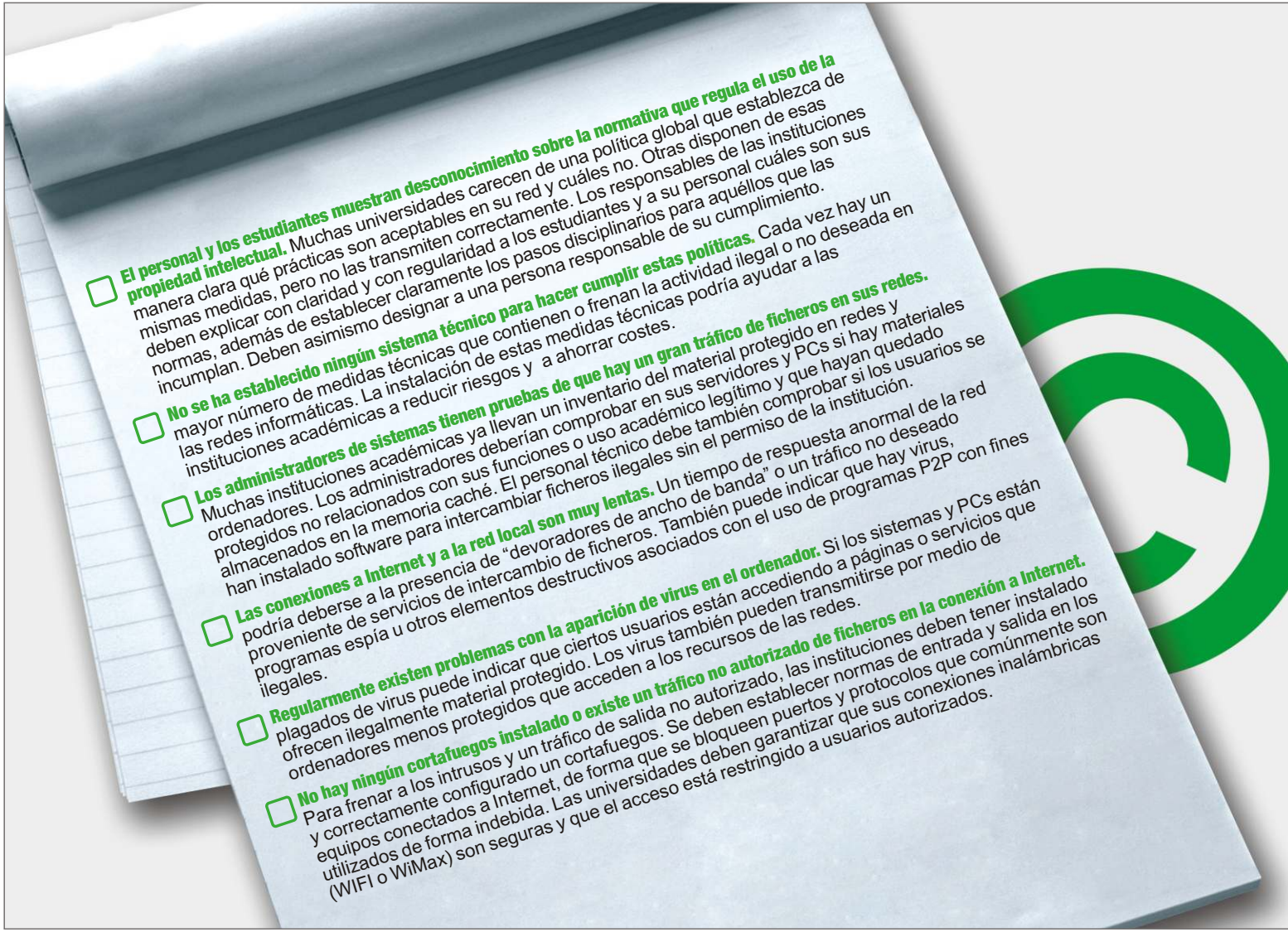
La música, las películas y otros ficheros protegidos sin licencia pueden consumir en exceso los giga bites en servidores y discos duros, aumentando los costes de almacenaje de datos de la institución. Normalmente el intercambio de ficheros consume una gran parte de la red de la institución académica y del ancho de banda de Internet, negando el acceso a los usuarios legítimos y reduciendo la productividad académica.

Piratas informáticos

Los recursos del ordenador instalado en una institución académica a veces son pirateados por personas de dentro y de fuera para acceder a su contenido y ficheros personales o para establecer servicios ilegales de distribución de música. Esta situación va desde simplemente colocar ficheros de música en una página web pública a piratear aquellos servidores cuyos puertos no están siendo utilizados y cuyos servicios no se han protegido lo suficiente.

La presencia de uno o varios de estos indicios puede ser indicativa de la necesidad de actuar contra los abusos de los derechos de propiedad intelectual.

¿CUÁNDO HAY QUE ESTAR ALERTA? ©



- **El personal y los estudiantes muestran desconocimiento sobre la normativa que regula el uso de la propiedad intelectual.** Muchas universidades carecen de una política global que establezca de manera clara qué prácticas son aceptables en su red y cuáles no. Otras disponen de esas mismas medidas, pero no las transmiten correctamente. Los responsables de las instituciones deben explicar con claridad y con regularidad a los estudiantes y a su personal cuáles son sus normas, además de establecer claramente los pasos disciplinarios para aquéllos que las incumplan. Deben asimismo designar a una persona responsable de su cumplimiento.
- **No se ha establecido ningún sistema técnico para hacer cumplir estas políticas.** Cada vez hay un mayor número de medidas técnicas que contienen o frenan la actividad ilegal o no deseada en las redes informáticas. La instalación de estas medidas técnicas podría ayudar a las instituciones académicas a reducir riesgos y a ahorrar costes.
- **Los administradores de sistemas tienen pruebas de que hay un gran tráfico de ficheros en sus redes.** Muchas instituciones académicas ya llevan un inventario del material protegido en redes y ordenadores. Los administradores deberían comprobar en sus servidores y PCs si hay materiales protegidos no relacionados con sus funciones o uso académico legítimo y que hayan quedado almacenados en la memoria caché. El personal técnico debe también comprobar si los usuarios se han instalado software para intercambiar ficheros ilegales sin el permiso de la institución.
- **Las conexiones a Internet y a la red local son muy lentas.** Un tiempo de respuesta anormal de la red podría deberse a la presencia de "devoradores de ancho de banda" o un tráfico no deseado proveniente de servicios de intercambio de ficheros. También puede indicar que hay virus, programas espía u otros elementos destructivos asociados con el uso de programas P2P con fines ilegales.
- **Regularmente existen problemas con la aparición de virus en el ordenador.** Si los sistemas y PCs están plagados de virus puede indicar que ciertos usuarios están accediendo a páginas o servicios que ofrecen ilegalmente material protegido. Los virus también pueden transmitirse por medio de ordenadores menos protegidos que acceden a los recursos de las redes.
- **No hay ningún cortafuegos instalado o existe un tráfico no autorizado de ficheros en la conexión a Internet.** Para frenar a los intrusos y un tráfico de salida no autorizado, las instituciones deben tener instalado y correctamente configurado un cortafuegos. Se deben establecer normas de entrada y salida en los equipos conectados a Internet, de forma que se bloqueen puertos y protocolos que comúnmente son utilizados de forma indebida. Las universidades deben garantizar que sus conexiones inalámbricas (WIFI o WiMax) son seguras y que el acceso está restringido a usuarios autorizados.

Las universidades pueden tomar medidas para frenar las infracciones contra los derechos de propiedad intelectual en sus redes.

PAUTAS PARA RESPETAR LOS DERECHOS DE PROPIEDAD INTELECTUAL ©

1 ESTABLECER UNA POLÍTICA EN MATERIA DE PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Y TRANSMITIRLA CORRECTAMENTE.
El personal y los estudiantes de estas instituciones deben entender que la copia ilegal y la transmisión de música, películas y obras de otras personas se considera una infracción contra el derecho de propiedad intelectual que la universidad no admite y que conlleva responsabilidades de tipo legal y económico. Estas medidas se pondrían mejor en práctica si se elaborara un código de conducta que las plasmara. Un modelo útil es el que existe en el Reino Unido, donde la política que define quién puede conectarse y utilizar JANET (Joint Academic NETwork of UK education, Red Académica Conjunta del sistema educativo del Reino Unido) está depositada en el JISC (Joint Information Systems Committee, Comité Conjunto de Sistemas de Información).
Visite:**www.ukerna.ac.uk/services/publications/policy/aup.html**
Esta política debe detallar claramente los distintos comportamientos inaceptables en las redes de las instituciones académicas, en sus aulas, campus y residencias, entre ellos el software para intercambio de ficheros ilegales, y dejar claras las sanciones establecidas. En este folleto se incluyen modelos de memorando y de código de conducta. Debe informarse correctamente sobre ellos al personal y a los estudiantes, por ejemplo:

- Poniendo a su disposición estas medidas directamente con su solicitud de ingreso, en el paquete de folletos de bienvenida. También tiene que estar fácilmente accesible en su página web.
- Asegurándose de que los estudiantes firmen un documento en el que acepten estas condiciones antes de ser autorizados a utilizar la red informática local.
- Los máximos responsables de la institución enviarán recordatorios periódicamente por e-mail.

2 COMPROBACIONES DEL SISTEMA. Muchas instituciones ya realizan auditorias de sus sistemas para localizar ciertos tipos de materiales protegidos, en particular software. Los inventarios deben incluir música, películas y cualquier otro material relevante protegido. Los archivos de música tienen normalmente un tamaño de 3 a 5 MB, almacenados en formatos .mp3, .wma, .ogg, .flac o .wav y que se suelen localizar en los directorios \Mi música o \Archivos Compartidos. Cada vez más a menudo, los archivos de música también se distribuyen como álbumes completos y se almacenan en formato .zip [o .rar]. Los archivos de películas normalmente tienen un tamaño de 500 a 700 Mbs, almacenados en formato .avi, .mpg o .mov. Algunas veces estos archivos se pueden comprimir en archivos del tipo .zip o .rar.

3 ELIMINACIÓN DEL MATERIAL PROTEGIDO ILEGAL. Las instituciones deben comprobar que cualquier copia de música comercial que se encuentre en sus sistemas es legal. Excusas del tipo "copia privada", "uso académico", "uso legítimo", "copia de evaluación" u otras no autorizan el almacenamiento o transmisión de bibliotecas de grabaciones comerciales en los sistemas de las instituciones académicas.

4 CONTROL DEL INTERCAMBIO DE FICHEROS. Prohibir la instalación de software no autorizado y el intercambio de ficheros en los sistemas de las universidades es una forma de reducir los problemas de seguridad y del material protegido, ya que se frena la gran mayoría de la piratería de contenidos antes de que se produzca. También existen medidas tecnológicas que pueden ayudar a las instituciones académicas a enfrentarse al uso indebido de material protegido. Por ejemplo, un sistema basado en una red local desarrollado por Red Lambda es el denominado cGrid **(www.redlambda.com\products_overview.htm)** del que ha sido pionera la Universidad de Florida en los Estados Unidos. Las universidades pueden personalizar este sistema para efectuar un bloqueo completo o selectivo, y asimismo se puede ofrecer una amplia gama de otros elementos relacionados con la gestión de la seguridad. Otra opción es instalar un sistema de filtrado en la red. Las grabaciones no autorizadas pueden ser identificadas dentro del tráfico de los archivos P2P y bloqueadas una a una, sin afectar al tráfico de otros archivos. La aplicación "Copysense" de Audible Magic **(www.audiblemagic.com)** es una de estas tecnologías.

5 CONFIGURACIÓN DEL CORTAFUEGOS. Los cortafuegos también pueden ser herramientas útiles para restringir el uso excesivo de ancho de banda que se produce como consecuencia de los P2P. Se pueden bloquear direcciones concretas de Internet, puertos o protocolos en los que normalmente se producen los intercambios de ficheros. La mejor práctica de seguridad es cerrar en el cortafuegos todos los puertos que no sean específicamente necesarios para las actividades de Internet autorizadas. También existen programas sofisticados que pueden bloquear o filtrar selectivamente el material protegido que pasa de Internet a la infraestructura local de la institución. Muchas instituciones académicas instalan ya de forma habitual tales programas junto con los filtros para bloquear virus, programas espía, anti-spam y e-mails nocivos.

6 CONTROL DE ACCESO A LAS REDES INALÁMBRICAS. Una institución académica debe garantizar que las conexiones inalámbricas a su red y a Internet sean seguras y estén encriptadas, de modo que estas conexiones no se puedan utilizar con fines ilegales. El software del servidor de conexiones inalámbricas permite configurar códigos de acceso y el nivel de encriptación deseado.

7 VIGILAR LOS NIVELES DE TRÁFICO. Los programas de gestión de la red, que se facilitan con el propio equipo, permiten a las instituciones comprobar si los usuarios y sus ordenadores están devorando ancho de banda y pueden configurarse de modo que prohíban, temporal o permanentemente y de forma automática, el acceso a ciertos usuarios. El personal técnico debe controlar las "zonas calientes o puntos negros" de tráfico para ver si hay un problema en el sistema o bien se está desarrollando una actividad ilegal.

8 MANTENER LA PROTECCIÓN ANTIVIRUS. El software antivirus puede filtrar y eliminar aquellos archivos que contienen virus, programas espía u otro material dañino, y debe instalarse en cada uno de los ordenadores. Los fabricantes de este tipo de software lo actualizan con regularidad para incluir nuevos virus. Las instituciones deben asegurarse de que todas las actualizaciones de antivirus se ejecutan con regularidad.

9 MANTENER LA PROTECCIÓN CONTRA PROGRAMAS ESPÍA. Existen programas de software capaces de encontrar y eliminar archivos espías, de spam y similares en los ordenadores de estas instituciones. Los programas antiespía deben instalarse y actualizarse con regularidad.

10 DESIGNAR A UN RESPONSABLE PARA EL CUMPLIMIENTO DE LAS NORMAS SOBRE MATERIAL PROTEGIDO. Alguien dentro de la propia institución debe ser responsable del cumplimiento de las normas sobre material protegido. Esta persona debe tener un puesto importante dentro de la organización, por ejemplo, un jefe de informática o un director financiero, ya que tendrá que encargarse de hacer cumplir el código de conducta de la institución académica, de eliminar el material ilícito con prontitud y de poder enviar avisos y tomar medidas disciplinarias en caso necesario.

MODELO DE MEMORANDO ©

Puede descargar una copia del memorando y del código de conducta en www.promusicae.es, www.egeda.es, www.sgae.es, www.fap.org.es y www.aie.es

MEMO

A:	(LISTA DE DISTRIBUCIÓN)
DE:	MÁXIMO RESPONSABLE DE LA INSTITUCIÓN ACADÉMICA
ASUNTO:	CÓDIGO DE CONDUCTA SOBRE EL USO DEL MATERIAL PROTEGIDO POR DERECHOS
FECHA:	(INSERTAR)

Nuestra universidad tiene una gran preocupación por evitar que sus redes informáticas se utilicen indebidamente para infringir derechos de propiedad intelectual.

El fin de esta carta es recordarte que (nombre de la institución) ha establecido un código de conducta sobre el uso del material protegido en sus redes, ordenadores y demás equipos informáticos.

Salvo que se tenga el permiso de los titulares de derechos, la difusión y copia del material protegido, incluso en Internet, que no sea para uso académico o uso personal exclusivamente, es ilegal y puede exponerte tanto a ti como a (nombre de la institución) a responsabilidades civiles y penales, según la legislación en materia de propiedad intelectual. Esto es aplicable a todo tipo de material protegido por derechos, entre los que se encuentran música, películas, juegos, software y otras obras.

Aquellas personas que han sido sorprendidas difundiendo ilegalmente material protegido tuvieron que enfrentarse a acciones legales y pagar miles de euros (libras o dólares en otros casos) como indemnización por daños y perjuicios.

El personal laboral y los estudiantes no deben colocar copias no autorizadas del material protegido en las redes, ordenadores, o demás equipos propiedad de (nombre de la institución).

Tampoco podrán colocar material protegido o involucrarse en actividades tales como el intercambio de ficheros no autorizados en redes P2P que puedan constituir un delito o conducir a cometerlo.

Se adjunta el código de conducta de (nombre de la institución) sobre el uso del material protegido, que incluye posibles medidas disciplinarias en caso de incumplimiento. (Nombre de la persona responsable del cumplimiento de este código) es el responsable de garantizar su cumplimiento y de eliminar aquellos archivos ilegales que se encuentren.

El incumplimiento de este código de conducta tendrá como consecuencia acciones disciplinarias y se te podría prohibir el uso de las redes informáticas de (nombre de la institución).

Por favor, no dudes en ponerte en contacto con (nombre del responsable del cumplimiento del código de conducta) si tienes alguna duda.

MODELO DE CÓDIGO DE CONDUCTA©

Este código de conducta debe ser explicado con claridad como parte integrante de la política del departamento de informática de una institución.

Consulte en www.wolfson.cam.ac.uk/facilities/computers/netuse/ los enlaces en inglés "Guidelines for Internet Use" y "Aceptable Use Policy" establecidos por el Wolfson College.

CÓDIGO DE CONDUCTA SOBRE EL USO DE MATERIAL PROTEGIDO

Nuestra universidad tiene una gran preocupación por evitar que sus redes informáticas se utilicen indebidamente para infringir derechos de propiedad intelectual.

(Nombre de la institución) considera importante la necesidad de respetar los derechos de propiedad intelectual en la creación y difusión de materiales protegidos, como música, películas, software y otras obras literarias, artísticas y científicas.

También nos preocupa que el uso indebido de tu ordenador o de la red de (nombre de la institución) pueda crearte problemas con la Ley, o abrir brechas de seguridad que puedan afectar a tu trabajo y al de tus compañeros estudiantes y profesores.

Ésta es la razón por la que (nombre de la institución) ha creado un conjunto de normas que deberás suscribir para conectarte a esta red.

El personal laboral de (Nombre de la institución) y sus estudiantes NO:

- Crearán, almacenarán ni pondrán a disposición de terceros copias de material protegido en los sistemas, equipos o medios de almacenamiento de (nombre de la institución), salvo que se haya obtenido expresamente autorización por escrito de los correspondientes titulares de derechos.
- Colgarán, almacenarán o pondrán a disposición de terceros copias no autorizadas de material protegido a través de la red local de (nombre de la institución) o de Internet utilizando los sistemas, equipos o medios de almacenamiento de (nombre de la institución), salvo que se haya obtenido expresamente autorización por escrito de los correspondientes titulares de derechos.
- Contribuirán o participarán en cualquier infracción de los derechos de propiedad intelectual utilizando o conectándose a una red de intercambio de ficheros, o utilizando un índice o servidor de P2P, con los sistemas o equipos de (nombre de la institución) en el área del campus o en sus residencias.

El responsable del cumplimiento de este código de conducta es (Nombre del responsable de hacer cumplir este código de conducta). La única excepción a estas normas es el uso de materiales protegidos por parte del personal con fines docentes, siempre dentro de los límites que establece la legislación en materia de propiedad intelectual.

Cualquier duda acerca de si un estudiante o un miembro del personal puede copiar o utilizar materiales protegidos de las distintas maneras expuestas en este código de conducta deberá consultarse a la persona responsable del cumplimiento de estas normas.

Los equipos informáticos del personal y de los estudiantes de (nombre de la institución) que contravengan este código de conducta podrán ser desconectados de forma temporal o permanente de su dirección IP [y/o clavija de acceso a la red]; además se les cobrarán los gastos ocasionados. También se les podrá abrir un proceso disciplinario que podría consistir en una prohibición permanente de utilización de las instalaciones informáticas y redes de (nombre de la institución).

Se retirará de forma inmediata cualquier material que viole este código de conducta.

_____

Firma y fecha

DESCARGA COMPLETADA 100%

PROMUSICAE
Productores de Música de España
Orense, 34- 8ª Planta
Edificio Iberia Mart II
28020 Madrid

Tlf. 91 417 04 70
Fax: 91 556 92 72
www.promusicae.es

AIE
Artistas, Intérpretes o Ejecutantes,
Entidad de Gestión de España
Príncipe de Vergara, 9
28001 MADRID

Teléfono: 91 781 98 50
Fax: 91 781 95 50
www.aie.es

EGEDA
Entidad de Gestión de Derechos
de los Productores Audiovisuales
Luis Buñuel, 2 - 3º
Edificio Egeda
Ciudad de la Imagen
Pozuelo de Alarcón
28223 Madrid

Tlf.: 91 512 16 10
Fax: 91 512 16 19
www.egeda.es

SGAE
Sociedad General de Autores y Editores
Fernando VI, 4
28004 Madrid

Tlf.: 91 3197477
www.sgae.es

FAP
Federación para la Protección
de la Propiedad Intelectual
Alfonso XII, 8 - 5º izq.
28014 Madrid

Tlf.: 91 522 46 45
Fax: 91 521 37 42
www.fap.org.es

AGEDI
Entidad de Gestión de Derechos
Intelectuales
Orense, 34- 8ª Planta
Edificio Iberia Mart II
28020 Madrid

Tlf.: 91 417 04 70
Fax: 91 556 92 72
www.agedi.es

Published by IFPI, March 2007