Pontificia Universidad Católica de Chile

Normativa de uso de Recursos Informáticos en la UC

Preparado por	:	Dirección de Informática
Versión	:	1.2
Fecha	:	Noviembre 2011

CONTENIDOS

1 INTRODUCCIÓN

1.1 PROPÓSITO

Este documento constituye la normativa de la Pontificia Universidad Católica de Chile respecto de la administración y uso responsable de los recursos informáticos, es decir, las redes de computadores, todos los computadores y dispositivos conectados a esas redes y a los recursos de la UC que con ellos se puedan acceder.

1.2 APLICABILIDAD

Esta normativa se aplica a todos los usuarios de los recursos computacionales de la Universidad, incluyendo a estudiantes, académicos, personal administrativo y a cualquier otra persona a quien se le facilita el uso de estos recursos, normando así todo tipo de uso de la plataforma informática.

Esta normativa se aplica a todos los computadores, sistemas de comunicaciones, periféricos, software, teléfonos y otros sistemas de funcionalidad similar que pertenezcan a la Pontificia Universidad Católica de Chile, o que utilice la infraestructura de la Universidad.

2 NORMA DE USO DE RECURSOS INFORMÁTICOS UC

2.1 RESPONSABILIDAD DE LA NORMA

La unidad responsable de la supervisión del cumplimiento de esta norma es la Vicerrectoría Económica y de Gestión (VREG).

El directivo responsable es el Director de Informática, quien creará los mecanismos necesarios para supervisar la aplicación de estas normas, velará por su cumplimiento, resolverá solicitudes y apelaciones de excepción y recomendará cambios a esta norma, según sea necesario.

Esta norma se revisará anualmente, y en el caso que se propongan cambios, éstos serán autorizados por el ***Comité Directivo del Rector***. Las unidades de la Universidad que tengan la capacidad podrán establecer normativas internas complementarias a esta, estableciendo detalles y características propias de su quehacer, respetando las normas generales de la Universidad aquí establecidas.

2.2 DERECHOS DE LOS USUARIOS

La Universidad entregará a la comunidad universitaria los recursos informáticos necesarios para apoyar su misión, a través de las actividades de docencia, investigación, extensión y administración. Estos recursos contemplan equipos de trabajo, acceso a las redes informáticas, software y cuentas de acceso a servicios centrales, como correo electrónico y sistemas de información.

Mediante estos recursos se facilitará el acceso de la comunidad UC a los recursos globales de la información, así como la capacidad de comunicarse con otros usuarios a nivel mundial. Con estos fines, la Universidad apoyará el uso de la tecnología y la comunicación electrónica en armonía con su misión y valores, con respeto a la legislación vigente y enmarcada en el uso apropiado y ético.

Se considera que la información contenida y difundida a través de las estaciones de trabajo y otros recursos informáticos provistos por la Universidad es privada, por lo que sus dueños o responsables determinan los privilegios de acceso a los mismos.

La Universidad reconoce el uso que estudiantes, académicos y personal administrativo hacen, ocasionalmente, de estos recursos tecnológicos para fines personales, siempre que éste no sea excesivo, no tenga fines comerciales, no afecte las actividades de otros miembros de la comunidad UC, no interfiera o afecta la operación eficiente y segura de los recursos tecnológicos y que se enmarque dentro de las normativas de la Universidad.

2.3 DEBERES DE LOS USUARIOS

Los recursos informáticos que la Universidad pone a disposición de sus miembros deben ser utilizados por éstos para apoyar el cumplimiento de sus funciones o labores propias dentro de la institución. Los usuarios deben resguardar y asegurar el correcto uso de la información y de los medios informáticos a los cuales tienen acceso, cumpliendo con las leyes vigentes en estas materias, y con las normativas internas formuladas en este ámbito.

Cualquier utilización de los recursos informáticos de la Universidad que esté fuera de los objetivos o tareas propias de la institución se considerará como inapropiada.

Los recursos informáticos de la Universidad no deben ser utilizados con propósitos o en actividades ilegales, contrarias a la ética, deshonestas, que dañen la imagen o la reputación de la Universidad, que arriesguen a la Universidad de ser acusada legalmente o que afecten la seguridad o el nivel operativo de la plataforma informática.

Constituyen usos inapropiados todas las acciones que no cumplan los reglamentos de la Universidad y cualquier hecho que viole las leyes del Estado de Chile y que incluyen, entre otros, lo siguiente:

- Violación de esta normativa.
- Instalar, utilizar y/o almacenar software sin licencia válida. En especial lo indicado en la ley 17.336 referente a la utilización de software sin licencia.
- Re-venta de servicios, tales como web hosting, servicios de correo o mensajería electrónica o conexiones a Internet, utilizando la infraestructura de redes de la Universidad.
- Acceder o intentar acceder sin autorización y/o en forma maliciosa a los sistemas y recursos informáticos de la Universidad.
- Apropiarse o intentar apropiarse indebidamente de las claves de acceso de otros usuarios a sistemas y equipos.
- Acceder, enviar, almacenar o poner enlaces a material pornográfico.
- Enviar correo electrónico no deseado (SPAM). Se excluye los correos electrónicos oficiales que las unidades envían a sus comunidades internas, lo que no es considerado SPAM, siempre y cuando dichos correos sigan las recomendaciones detalladas en el punto 3.5: “Uso de correos masivos al interior de la Universidad”.

- Incurrir en cualquier hecho que viole las leyes vigentes del Estado de Chile, especialmente, ley relativa a los Delitos Informáticos [19.223], la ley sobre Protección de la Vida Privada [19.628], la ley sobre Delitos de Pornografía Infantil [19.927] y la ley de Propiedad Intelectual [17.336].

- Provocar denegación de cualquier servicio de la red, dispositivos de comunicaciones, servidores, tanto de la Universidad como de entidades externas.

- Instalar y ejecutar servidores o software que se utilicen para el acceso inapropiado o no autorizado de terceros a la Universidad a material propio de ésta.

- Violación de la Norma Específica sobre el Uso del Correo Electrónico.

- Sobre utilizar la plataforma tecnológica en desmedro de otros integrantes de la comunidad UC, por ejemplo, utilización excesiva del ancho de banda o apropiarse mediante el uso de software de descarga Peer-to-Peer, del acceso a internet o cualquier tramo de la red UC.

- Cargar en forma intencional o negligente y/o no reportar a la Dirección de Informática, o al responsable de redes de la unidad académica, la existencia de archivos que contengan virus, caballos de troya (“troyanos”), gusanos (“worms”), archivos dañinos o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos, de la red o de propiedad de terceros o provocar que el recurso computacional realice funciones para las cuales no fue adquirido.

- Monitorear sin autorización el tráfico de cualquier red, sistema o computador, como también hacer escaneo de puertos. Se exceptúan de esta prohibición los responsables de las redes de las unidades, quienes podrán hacer estos monitoreos sólo al interior de su red.

- Violación o engaño de la seguridad de la red o de sistemas informáticos.

- Suplantar identidad de terceros, engañar o confundir sobre el origen de las comunicaciones u otro contenido.

- Revelar a terceros contraseñas de acceso o compartirlas con otros usuarios.

En caso de ser considerado necesario, toda la información contenida o difundida en los recursos computacionales y de comunicación provistos por la Universidad para sus distintos fines (académico, de investigación, administrativo, personal) es susceptible de auditoría e investigación por parte de la Dirección de Auditoría de la institución, de acuerdo a las normas y procedimientos establecidos.

2.4 APLICACIÓN DE LA NORMATIVA

El incumplimiento de esta normativa es considerado por la Universidad como un abuso. Considerando que el incumplimiento puede ir desde una falta leve hasta una transgresión grave, incluso con carácter de delito, la Vicerrectoría Económica y de Gestión (VREG) tomará las medidas disciplinarias que corresponda en cada caso.

Cualquier usuario o equipo que no cumpla con la normativa de uso de recursos informáticos será inhabilitado o desconectado de la red por personal de la Dirección de Informática, en coordinación con las unidades, y sólo se restituirán sus servicios una vez que se haya comprobado la solución a la causa de dicha medida.

3 NORMA ESPECÍFICA SOBRE EL USO DEL CORREO ELECTRÓNICO

3.1 USO DEL CORREO ELECTRÓNICO

La presente normativa tiene como objetivo regular el uso del sistema de correo electrónico que la UC pone a disposición de académicos, alumnos, personal administrativo y exalumnos, como herramienta de apoyo a la gestión, los procesos educativos y de comunicación en general. La Universidad se reserva el derecho de regular las condiciones, frecuencia y oportunidad de uso de la correspondencia electrónica y de aceptar o rechazar conexiones de correo electrónico desde cualquier dirección de correo electrónico o servidor externo.

Se hace notar expresamente que el correo electrónico normal (no encriptado ni firmado electrónicamente), NO es un medio seguro para transmitir información, ni tampoco permite asegurar la identidad de remitente. Si bien la Universidad toma los resguardos para proteger la confidencialidad, integridad y disponibilidad de los correos almacenados en los servidores institucionales del correo ***@uc.cl***, no puede garantizar la confidencialidad, seguridad y privacidad en la transmisión a través de la red.

3.1.1 Derechos de los usuarios

Todos los académicos, alumnos y funcionarios de la Universidad, como también los exalumnos egresados tienen derecho a una casilla de correo electrónico ***@uc.cl***.

También tienen derecho a una cuota de disco para almacenamiento de los correos electrónicos, cuya capacidad será determinada por la Dirección de Informática dependiendo de la disponibilidad de recursos de almacenamiento.

Los usuarios de correo ***@uc.cl*** tienen derecho a la privacidad de sus correos electrónicos, en los términos que se detallan en los párrafos siguientes.

Aquellos académicos o funcionarios que jubilen en la Universidad tendrán derecho a mantener su casilla de correo, asimismo los alumnos que egresen de alguna de las carreras de pregrado o postgrado, pasando a tener calidad de exprofesores, exfuncionarios y exalumnos respectivamente.

Los académicos y funcionarios que dejen de pertenecer a la UC, como también los alumnos que dejen la Universidad sin haber egresado, dejan de tener derecho a su casilla de correo electrónico ***@uc.cl.***

3.1.2 Uso apropiado

El Uso Apropiado del Correo Electrónico UC hereda lo definido en las Normativa de Uso de Recursos Informáticos de la Universidad Católica de Chile. Cualquier otro uso no enunciado es considerado inapropiado.

3.1.3 Uso inapropiado

A continuación se explicitan algunas prácticas y usos inapropiados del correo electrónico, sin que se limiten sólo a las señaladas:

- Utilizar el correo electrónico para fines comerciales o de ganancias monetarias personales, que no estén relacionadas directamente con las actividades de la Universidad.

- Brindar servicios que, de manera directa o indirecta, faciliten la proliferación de SPAM o "correo electrónico masivo no solicitado". En esto se incluye casillas de correo, software para realizar SPAM, hosting de sitios de Web para realizar SPAM o que realicen SPAM.

- Enviar un alto número de mensajes en intervalos cortos de tiempo con el fin el dificultar o paralizar el servicio de correo electrónico de la UC o terceros.

- Utilizar servidores de correo externos, estaciones de trabajo de usuario y en general cualquier recurso que no sea el dispuesto por la UC para emitir correo con identificación de dominios UC (ejemplo: @uc.cl, @vra.uc.cl).

- Habilitar servidores o levantar servicios de correo no acordados con la Dirección de Informática, utilizando equipos o las redes de comunicaciones provistos por la Universidad.

- Enviar contenidos en los correos electrónicos contrarios a las disposiciones del Orden Público, la moral, las buenas costumbres nacionales e internacionales, los usos y costumbres aplicables en Internet y el respeto de los derechos fundamentales de las personas.

- Enviar con contenido ilegal de manera intencionada. Ejemplos: programas piratas, pornografía infantil, amenazas, estafas, virus o código hostil en general.

- Enviar correos electrónicos con contenido que constituyan acoso, amenazas o menoscabo de terceros.

- Enviar de correo electrónico haciendo proselitismo político.

- Enviar mediante correo electrónico cualquier tipo de publicidad o cualquier tipo de aviso comercial no solicitado previamente por el destinatario.

- Alterar encabezados de correos electrónicos creando falsificaciones de estos, falsificar nombres de dominios, o cualquier otra forma de enviar correo electrónico engañoso.

- Acceder en forma no autorizada a correos electrónicos dirigidos a otras personas.

- Falsificar encabezados para hacerse pasar por otra persona (spoofing). Se aclara que el uso de apodos anónimos no constituye la personificación.

- Enviar mediante correo electrónico de toda cadena de correos, hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "Cartas en Cadena", "Pirámides", "Phishing" o enviar correo electrónico solicitando donaciones caritativas, peticiones de firmas o cualquier material relacionado.

3.2 CONSIDERACIONES DE PRIVACIDAD

El contenido de toda casilla de correo electrónico que esté directamente vinculada a una persona específica se considera *correspondencia privada*.

Por otra parte, se considera que toda casilla de correo electrónico donde la dirección de correo electrónico es de carácter genérico (alias de correo), es decir, asociado a un servicio, propósito, unidad, función específica, etc. (ejemplo: 5555@uc.cl, contacto@uc.cl), no tendrá el carácter de correspondencia privada ya que no está asociada a una persona en particular y por esto, los correos electrónicos recibidos podrán ser automáticamente dirigidos a un grupo de personas que la UC estime conveniente para el desarrollo de dicho propósito o función.

Así mismo, la correspondencia electrónica pierde el carácter de privada en su origen cuando es enviada con copia a alguna dependencia o unidad de la Universidad. Sin embargo, lo anterior no restringe el carácter de privado en la correspondencia recibida, la cual siempre será considerada como tal[1]. Por lo tanto

[1] Ver Dictamen 260/19 de Enero de 2002 emitido por la Dirección del Trabajo. (http://www.dt.gob.cl/legislacion/1611/article-63171.html)

y resumiendo lo anterior se considera la comunicación de tipo privada, cuando el destinatario es individualizado por el emisor.

El emisor de un correo electrónico debe identificar sus datos (nombre, apellido, unidad interna a la que pertenece) para el conocimiento de los mismos por parte del destinatario.

3.3 RESPONSABILIDADES DE LA ADMINISTRACIÓN

Con el fin de enmarcar el ámbito de responsabilidad de los administradores del sistema de correo electrónico detallamos los siguientes puntos:

- El administrador de correo electrónico @uc.cl de cualquier servidor institucional de la UC no podrá, bajo ninguna circunstancia, leer, copiar, retener, desviar, divulgar o alterar correspondencia electrónica que no esté dirigida específicamente a su dirección, salvo que cuente con el expreso consentimiento del usuario destinatario de dicho correo electrónico. Se exceptúa de esta prohibición las técnicas, procedimientos y equipos de filtrado antispam.

- Todo mensaje que no pueda ser entregado a un destinatario, cualquiera sea la causa, deberá ser devuelto al emisor en forma automática por medio del sistema de correo, a excepción que este haya sido eliminado por los servicios de filtro de correos.

- El único fin con el que el administrador de un servicio de correo electrónico podrá copiar los correos electrónicos será el de “respaldo” o copia de seguridad. El contenido de los “respaldos” no podrá ser conocido por ninguna persona a excepción del usuario al que fue enviado dicho correo electrónico (destinatario), exceptuando los casos excepcionales en que la Universidad podrá acceder al contenido de la correspondencia, como los siguientes:

  i. Por voluntad de la persona, previamente autorizado por escrito.

  ii. Enfermedad definitiva o temporal que no le permita acceder a su correo electrónico. Esto deberá ser previamente autorizado por escrito.

  iii. Por requerimiento judicial.

- En caso de desvinculación(ej. retiro voluntario, despido, etc.) la persona que no tenga derecho a conservar su casilla @uc.cl contará con un tiempo de 2 semanas para traspasar sus correos. Luego de ese tiempo, la casilla será eliminada por el administrador de correo electrónico.

3.4 LIMPIEZA DE CASILLAS

La limpieza de correos antiguos es un proceso necesario para asegurar un adecuado funcionamiento y disponibilidad de los servicios para todos. A todos los usuarios se les recomienda que almacene localmente sus correos, esto es, en su computador personal o en otro medio, en forma constante.

La Universidad no borrará los mensajes de correo de usuarios que utilicen el servicio en forma constante. Si un usuario no accede a su correo durante 6 meses, se eliminarán los mensajes que a la fecha tenga en su casilla, previa notificación a través del mismo correo @uc.cl o por otros medios que estén al alcance de la Universidad y su cuota se reducirá al 10% de la cuota normal asignada. Si vuelve a utilizar el servicio, la cuota será restablecida al 100%.

3.5 USO DE CORREOS MASIVOS AL INTERIOR DE LA UNIVERSIDAD

Un correo masivo es un correo que se envía simultáneamente a un gran número de destinatarios.

El envío de correos masivos a usuarios de una unidad de la Universidad, debe estar autorizado por las autoridades de dicha unidad. En el caso que se considere el envío de correos masivos a múltiples usuarios de otras unidades de la Universidad, los correos deben contar con la autorización expresa de la Vicerrectoría de Comunicaciones y Educación Continua.

3.5.1 Correos masivos autorizados

Se encuentran autorizados los correos masivos de una unidad a destinatarios de esa misma unidad.

> Ejemplo: Dirección de Asuntos Estudiantiles de la Facultad de Derecho a alumnos de la Facultad de Derecho.

También se encuentran autorizados los correos masivos de una unidad A a un conjunto de destinatarios B, siempre que la unidad A tenga como misión fundamental y específica prestar servicios a los destinatarios B.

> Ejemplo: DASE a alumnos beneficiarios de la Beca Padre Hurtado; DAP a todos los funcionarios.

En este caso, el mensaje debe contener información concreta relativa a estos servicios.

Asimismo, se encuentran autorizados los correos masivos de una unidad A a un conjunto de destinatarios B, siempre que entre ambos exista un vínculo evidente.

Ejemplo: Facultad de Física a sus ex alumnos.

Por último, se encuentran autorizados los correos masivos de una unidad A a un conjunto de destinatarios B, que contengan encuestas o estudios de opinión, siempre que estos estudios estén autorizados por las autoridades de la Dirección Superior o de las Facultades correspondientes.

En todos los casos anteriores, se solicita en lo posible aplicar las recomendaciones detalladas en el Anexo de esta norma: “Buenas prácticas antes de enviar un correo masivo”.

3.5.2 Correos masivos no autorizados

No se encuentran autorizados los correos masivos de una unidad A a un conjunto de destinatarios B cuando la unidad A no tiene como misión fundamental y específica prestar servicios a los destinatarios B.

Ejemplo:

De: Ediciones ARQ

A: Académicos UC

Asunto: Venta especial de libros Ediciones ARQ.

4 NORMAS DE ACCESO A INTERNET

4.1 ACCESO PARA USUARIOS

La Dirección de Informática administrará el ancho de banda de acceso a internet realizando una segmentación de servicios para la comunidad UC y administrará las medidas de seguridad al interior de la Universidad.

La normativa contempla el acceso a los servicios de Internet que permiten el desarrollo de las funciones propias de la comunidad UC, siempre y cuando no causen perjuicios al normal funcionamiento de la Red UC y se enmarquen en los usos aceptables indicados en la sección 2. Lo anterior se traduce en que los usuarios pueden navegar por sitios web de la UC e Internet, entre otros protocolos y aplicaciones.

Solo se podrán realizar conexiones desde el exterior (Internet) hacia estaciones de trabajo de usuarios ubicadas dentro de la red UC mediante el servicio VPN ofrecido por la Dirección de Informática. Hacerlo de manera directa implica un riesgo de seguridad muy alto que podría afectar a un gran número de computadores de la red UC.

El envío de correo usando servidores externos se permite a través del protocolo estándar Submission (tcp/587). El acceso a servidores SMTP (25/tcp) y SMTP+SSL (465/tcp) externos solo se permite a los servidores institucionales debidamente registrados. La UC cuenta con una plataforma de correos y servidores que ofrece el servicio a toda la comunidad UC, por lo que el envío de correos @uc.cl debe usarse a través de este servicio.

4.2 ACCESO PARA SERVIDORES

Si un servidor ofrece algún servicio a público ubicado al exterior de la Universidad y requiere ser visible desde todo Internet, se deberá declarar al área de seguridad informática de la Dirección de Informática su objetivo y solicitar la creación de reglas de acceso para su funcionamiento. El funcionamiento correcto y seguro es de responsabilidad de la unidad solicitante.

4.3 ACCESOS ESPECIALES

En casos en que se requiera de accesos especiales, éstos deberán ser acreditados con la Dirección de Informática y siempre que se cumpla con los fines declarados anteriormente en la presente norma.

5 NORMAS DE USO DE REDES INALÁMBRICAS

Las redes inalámbricas presentan varias ventajas de utilización al permitir gran movilidad y comodidad de conexión a las redes. Para garantizar la coordinación técnica necesaria que requiere una red inalámbrica para la Universidad, se establece que la Dirección de Informática será el único responsable del despliegue y la gestión de los estándares inalámbricos 802.11 y puntos de acceso de las dependencias de la Universidad. Las unidades deberán usar protocolos inalámbricos 802.11 (o sus relacionados) con puntos de acceso inalámbricos en coordinación con la Dirección de informática.

Las redes inalámbricas están basadas en el estándar IEEE 802.11, que es por naturaleza fácil de implementar, pero muy sensible a la superposición de frecuencias y amenazas de seguridad. Debido a estas características, todo uso inalámbrico debe ser planificado, implementado y gestionado de una manera muy cuidadosa y con una coordinación central para garantizar la funcionalidad básica, máximo ancho de banda y un uso seguro.

La actual tecnología inalámbrica 802.11 despliega una señal de muy baja potencia en una banda de frecuencia dividida en donde sólo 3 canales pueden operar simultáneamente. El propósito principal de estos canales no es ofrecer redes por separado, sino garantizar que los puntos de acceso adyacentes con un ligero solapamiento puedan realizar cobertura de áreas que no se interfieren entre sí. En el caso normal, es necesario utilizar los tres canales de una manera integrada como una red unificada a fin de lograr un diseño óptimo. Por ello no es posible permitir a los particulares que instalen sus propios puntos de acceso sin una coordinación centralizada, debido a la interferencia de la señal resultante y su degradación en el rendimiento a la red inalámbrica común.

6 INCIDENTES

Todo miembro de la comunidad UC tiene el deber de informar cualquier evento sospechoso que implique algún uso inapropiado de los recursos computacionales, como por ejemplo:

- Estaciones de trabajo de usuarios con comportamiento extraño o claramente comprometidas.
- Detección de extracción de información o sospecha de la misma.
- Detección de infección (virus electrónico) de equipos.
- Detección de SPAM causado por recursos internos.

Cualquier incidente que ponga en riesgo la seguridad de la información o de los servicios UC debe ser informado al departamento de Soporte de la Dirección de Informática, en el anexo 5555 o a la casilla 5555@uc.cl o al área de soporte de informática de la unidad, si ésta cuenta con un área propia.

7 SANCIONES

Debido al riesgo al que se expone la Universidad, la autoridad superior será informada de cualquier práctica ilícita o contraria a esta normativa, por lo cual se podría disponer de sanciones administrativas hacia la persona directamente responsable, según dicta el Código del Trabajo Art. 154 inciso 10 y la normativa interna de la Universidad.

Respecto al incumplimiento de la ley 17.336 de propiedad intelectual, sea por la utilización de software sin licencia u otros, se establece que todas las responsabilidades que de ellas deriven, serán asumidas en su totalidad por la persona que cometa la infracción.

Estaciones que sean detectadas con problemas de seguridad, daño a lo instalado o intento de dañar otras estaciones de trabajo, serán intervenidas y bloqueadas hasta que la situación sea corregida. Se podrán realizar las siguientes acciones sobre la estación vulnerable o peligrosa:

- Bloquear, si es necesario.
- Revisar.
- Reparar.
- Desbloquear, si corresponde.

Una vez que se identifica una vulnerabilidad en la estación de trabajo, ésta perderá su calidad de objeto confiable, por lo tanto, perderá los accesos a los recursos informáticos de la UC con los que cuenta la estación en cuestión.

8 DOCUMENTACIÓN COMPLEMENTARIA

Documentación complementaria a este documento se detalla en la siguiente lista de documentos:

Ley 17.336 sobre Propiedad Intelectual.

Ley 19.223 sobre Delitos Informáticos.

Ley 19.628 sobre Protección de la vida privada.

Dictamen Nº 260/19 de 2002. Procedencia del acceso a correspondencia electrónica.

Documento: “Prácticas de Escritorio Limpio”

Documento: “Condiciones de uso red inalámbrica UC”

Documento: “Buenas Prácticas antes de enviar un correo electrónico masivo”

9 GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Worm: Virus informático con la capacidad de distribuirse a sí mismo en una red sin la intervención de un ser humano.

Troyano: Virus informático que aparenta ser un programa inofensivo aunque de forma oculta realiza otras funciones.

Peer-to-Peer: Concepto que describe conexiones punto a punto. En este caso se llama a las tecnologías aplicadas a compartir información de cualquier tipo en Internet. Muchas aplicaciones utilizan estas tecnologías para transferir sin autorización software o contenido protegido por las leyes de propiedad intelectual provocando degradación en la calidad de las comunicaciones.

Usuario: Cualquier persona de la comunidad UC que utilice recursos informáticos, computacionales y de comunicaciones. Se extiende también a personas invitadas por algún integrante de la comunidad UC o que, circunstancialmente, se les autorice utilizar los recursos tecnológicos de la UC.

Comunidad UC: Todo integrante de los diferentes estamentos de la Universidad: académicos, alumnos, directivos, personal administrativo y profesional.