Reglamento para el uso de la red de cómputo del Instituto de Investigaciones Biomédicas de la UNAM

Introducción

El Instituto de Investigaciones Biomédicas de la UNAM proporciona servicios de cómputo con la finalidad de contribuir al buen desarrollo de las actividades académicas de investigación y enseñanza, así como de las actividades administrativas sobre las que se apoyan la docencia y la investigación, facilitando el intercambio y transformación de información. El Instituto da acceso a los servicios de cómputo a los miembros del personal académico y administrativo y a los estudiantes que así lo requieran, para la realización de sus actividades académicas y/o administrativas, y provee a los usuarios con una red interna de datos, con acceso a Internet, así como con un servicio de correo electrónico. La instalación y el mantenimiento de estos servicios requieren de una cantidad significativa de recursos, y por lo tanto se espera que los usuarios mantengan una conducta responsable cuando los utilicen. El presente documento establece las políticas de uso aceptable de los servicios de cómputo, a las cuales deben ajustarse los usuarios.

La utilización de estos servicios de cómputo conlleva la responsabilidad de aceptar las políticas de uso adecuado que se establecen en el presente documento.

1 Red interna de datos

1.1 Para acceder a la red interna es necesario obtener una clave de usuario y una contraseña. Esta clave debe ser conocida solamente por el usuario y es intransferible. En caso de cualquier olvido la única persona autorizada para proporcionar una nueva clave y/o contraseña es el administrador de la red. Si el usuario sospecha que algún otro usuario está haciendo uso de su clave debe reportarlo al administrador de la red. En ocasiones una clave de usuario y su respectiva contraseña pueden ser compartidas por varios usuarios pertenecientes a un mismo grupo. Es responsabilidad de los miembros de ese grupo no proporcionar su clave y contraseña compartida a ningún otro usuario.

1.2 Ningún usuario deberá permitir el acceso a la red interna del Instituto a personas externas al mismo o a personal no autorizado, mediante el uso de la cuenta que le ha sido asignada.

1.3 Los servicios de impresión en red deben ser utilizados únicamente para imprimir documentos relacionados con las labores académicas y administrativas del usuario.

1.4 Todos los usuarios de los servicios de cómputo deberán responsabilizarse de tener su información debidamente respaldada, y podrán hacer uso de sus unidades de red para este propósito, pero siempre dentro de sus cuotas de espacio en la red. Sin embargo, las unidades compartidas no podrán ser usadas

para este propósito.

1.5 Las unidades de red no se deberán utilizar para guardar archivos de música (mp3, wav, wma, etc.), o videos de uso personal (avi, mpg, wmv, mov, etc). Queda estrictamente prohibido tener imágenes o videos pornográficos, o software ilegal.

1.6 La información almacenada en las unidades de red se organizará en carpetas. Cada investigador tendrá una carpeta para su uso exclusivo, y cada grupo de investigación tendrá una carpeta para el uso compartido del grupo. Habrá un sistema de cuotas de espacio en estas unidades, y las cuotas serán fijadas por la Sección de Cómputo, de acuerdo al espacio total de almacenamiento disponible en la red de datos. Estas unidades serán respaldadas regularmente por la Sección de Cómputo.

1.7 Habrán también unidades de red para los diversos servicios y unidades administrativas del Instituto, y estas también estarán sujetas al sistema de cuotas y serán respaldadas regularmente.

1.8 Habrá una unidad compartida, que será designada la unidad R:, a la que tendrán acceso todos los usuarios de la red. Esta unidad tiene como propósito facilitar el intercambio de archivos e información entre los mismos usuarios de la red. La información de esta unidad será eliminada al día siguiente de su creación, y no será respaldada - pero no tendrá cuota. Todo archivo que no esté en una carpeta será borrado automáticamente.

2 Correo electrónico

2.1 Todos los Investigadores y Técnicos Académicos tendrán una cuenta de correo electrónico, así como todos los estudiantes en activo, que deberán solicitar su cuenta al administrador del sistema, con el aval del Coordinador de Enseñanza. Los Trabajadores Administrativos también podrán tener una cuenta, con el aval del Secretario Administrativo.

2.2 La cuenta de correo electrónico es personal e intransferible, por lo que la clave y contraseña para acceder al mismo deberán ser conocidas solamente por el usuario y no deberán ser compartidas con nadie, por lo que si se detecta que el servicio es utilizado por otra persona que no sea el titular se podrá cancelar el servicio.

2.3 El servicio de correo electrónico no deberá ser utilizado para enviar mensajes en forma masiva, o para enviar mensajes ofensivos o de hostigamiento a otras personas. Se prohíbe utilizar la cuenta de correo para enviar o reenviar mensajes que pertenezcan a “cadenas”. Queda estrictamente prohibido el uso de las cuentas para fines comerciales.

2.4 El usuario no debe utilizar la cuenta de correo para enviar o recibir archivos ejecutables que comprometan la seguridad del sistema. En caso de que sea necesario enviar o recibir datos adjuntos a un mensaje de correo electrónico el usuario tiene la responsabilidad de analizarlos para detectar la

posible presencia de virus informáticos, y cualquier posible infección debe ser reportada de inmediato al administrador.

2.5 El servicio de correo electrónico cuenta con un sistema de filtrado de virus. Todo usuario de correo electrónico que utilice una cuenta en un servidor de correo que no filtre el correo para eliminar virus deberá filtrar su correo electrónico a través del servidor de correo electrónico del Instituto, y la Sección de Cómputo tendrá la facultad de bloquear el acceso directo a servidores que no filtren su correo.

2.6 Queda prohibido tener servidores propios de correo. Asimismo queda estrictamente prohibido que el administrador del correo electrónico revise el correo de cualquiera de los usuarios del Instituto. El incumplimiento por parte del administrador de correo puede ocasionar la suspensión de sus funciones así como las sanciones que considere conveniente la Comisión de Cómputo.

3 Acceso a Internet

3.1 El acceso a Internet debe ser utilizado fundamentalmente para visitar sitios relacionados con actividades académicas. Se permite el uso personal siempre y cuando sea razonable y no comprometa de ninguna forma la seguridad de los servicios de cómputo del Instituto.

3.2 El acceso a Internet contará con restricciones para sitios inseguros, y será particularmente importante que los usuarios tengan un comportamiento responsable en aquellos sitios que no queden restringidos, ya que un uso inadecuado puede comprometer seriamente la seguridad de los servicios de cómputo, así como afectar el trabajo de otros usuarios del Instituto.

3.3 Queda prohibido el uso de programas para “bajar” o copiar de Internet archivos de procedencia no segura o ilegal, tales como aquellos que aparecen en el anexo 1. Por estos motivos también queda prohibido instalar y ejecutar programas que permitan el intercambio de archivos (anexo 2). Queda también prohibido utilizar los recursos de cómputo para actividades no académicas o de trabajo, como pláticas en línea o “chat”.

3.4 Se sugiere que se minimice o se evite la práctica de bajar e instalar programas gratuitos del Internet, tales como salvapantallas, pues estos frecuentemente instalan programas indeseables como espías.

3.5 Queda prohibida la instalación de servidores Web o páginas Web en las computadoras del Instituto, a excepción de aquellas que pertenecen al portal del Instituto. Queda prohibido además utilizar los servicios de cómputo del Instituto para realizar actividades comerciales

3.6 Todas las conexiones al Internet tendrán que estar dentro del Firewall para seguridad del sistema de red, a excepción de aquellas expresamente autorizados por la Comisión de Cómputo. Toda máquina con IP fuera del Firewall a la que se detecte algún incidente de seguridad podrá ser desconectada físicamente de la red en tanto se corrija el problema, y deberá ser nuevamente autorizada por la

Comisión de Cómputo para poder operar fuera del Firewall.

3.7 La Sección de Cómputo deberá configurar y certificar los equipos para que se puedan conectar a la red. Todo equipo que se vaya a conectar deberá contar con antivirus vigente y con las actualizaciones al sistema operativo que permitan asegurar que no existan vulnerabilidades que pongan en entredicho la integridad y seguridad de la red del Instituto.

3.8 Queda estrictamente prohibido cambiar el IP asignado o usar un IP que no haya sido asignado por la Sección de Cómputo. También está prohibido configurar equipos y conectarlos a la red sin que hayan sido revisados y certificados por la Sección de Cómputo. Lo anterior incluye la prohibición de instalar y configurar concentradores alámbricos. En caso de existir la necesidad de instalar puntos de acceso inalámbrico a la red, se deberá remitir una solicitud por escrito a la Comisión de Cómputo, para que personal de la Sección de Cómputo lleve a cabo las acciones necesarias para garantizar la seguridad de la red.

3.9 Las máquinas que estén dispersando virus deberán ser desconectadas de la red hasta que se resuelva el problema y los virus sean eliminados. Los usuarios que detecten virus en sus equipos deberán apagarlos y dar aviso a la Sección de Cómputo, que deberá darle máxima prioridad a la solución de este tipo de problemas.

3.10 La sección de cómputo no se hace responsable de problemas de comunicación con servidores externos por problemas en RedUNAM.

3.11 Es responsabilidad de los usuarios mantener actualizado tanto el sistema operativo con los parches de seguridad como el antivirus con las actualizaciones disponibles para este fin. Para ello, se sugiere que cada grupo de investigación tenga un responsable.

3.12 Cualquier excepción a los puntos anteriores puede ser válida siempre y cuando el usuario proporcione una clara justificación académica, excepto los puntos de prohibición estricta que no deberán ser transgredidos por ningún motivo.

4 Monitoreo

4.1 El Instituto se reserva el derecho de monitorear el uso de los servicios con el fin de detectar el posible mal uso de los mismos. Durante el monitoreo se tomarán todas las medidas necesarias para garantizar la privacidad del usuario. Por ningún motivo se examinará el contenido de comunicaciones individuales de correo electrónico.

4.2 En caso de sospechas de abuso por parte de algún usuario se le pedirá una explicación sobre la actividad detectada, lo cual se hará en estricta confidencialidad.

4.3 En caso de abusos reiterados por parte de algún usuario se podrá negar al mismo el uso de los servicios de cómputo del Instituto, por acuerdo de la Comisión de Cómputo.

5. Servicios de Computo

5.1 Toda solicitud de servicios de computo deberá hacerse a través de la página Web. Las cuestiones muy urgentes podrán ser atendidas mediante una llamada telefónica o una visita del interesado al taller de cómputo, pero en esos casos se deberá llenar la solicitud de servicio a la brevedad posible, y se exhorta a los usuarios de los servicios de cómputo a no usar este mecanismo mas que en casos verdaderamente excepcionales y a respetar la programación de los servicios de cómputo.

5.2 Cada grupo de investigación deberá tener un encargado de servicios de cómputo para tratar con él todo lo concerniente a los servicios de cómputo, y que esta sea la persona encargada de la aprobación de los servicios recibidos.

5.3 La Sección de Computo podrá canalizar órdenes de servicio a proveedores externos siempre que lo considere conveniente, pero en todos los casos deberá revisar primero el equipo de cómputo para evaluar la necesidad de enviarlo a un taller externo. Sin embargo, el usuario puede decidir enviar el equipo a reparación directamente sin que se requiera la participación de la Sección de Cómputo (por ejemplo, cuando haya una garantía vigente).

5.4 Cada grupo de investigación se hará responsable de los programas que se instalen en los equipos de computo que adquieran. La Sección de Cómputo solamente instalará programas de procedencia legal que cuenten con la licencia respectiva.

5.5 La Sección de Cómputo se reserva el derecho de desconectar equipos de la red y no realizar órdenes de servicio por mal uso de la computadora: equipo con programas inseguros de música o video, entrada repetitiva de virus a través de correo no filtrado, equipos operando sin antivirus actualizados o con sistemas operativos sin los parches de actualización. La Comisión de Cómputo deberá ser informada de estos casos.

Anexo 1.

Lista de extensiones de archivos permitidas solamente para actividades académicas

NOTA: Se puede monitorear para asegurar un uso académico legítimo.

ASF --> Windows Media

AVI--> BSPlayer

BIK --> RAD Video Tools

DIV --> DivX Player

DIVX --> DivX Player

DVD --> PowerDVD

IVF --> Indeo

M1V --> (mpeg)

MOV(*) --> QuickTime

MOVIE --> (mov)

MP2V --> (mpeg)

MP3 --> Música comprimida

MP4 --> (MPEG-4)

MPA --> (mpeg)

MPE --> (mpeg)

MPEG --> (mpeg)

MPG --> (mpeg)

MPV2 --> (mpeg)

QT --> QuickTime

QTL --> QuickTime

RPM --> RealPlayer

SMK --> RAD Video Tools

VIV --> Video VIV

WAV --> Música digital

WM --> Windows Media

WMA --> Música comprimida para Windows Media

WMV --> Windows Media

WOB --> PowerDVD

Anexo 2.

Lista de Programas para Intercambio de Música

3ECS

Adult Media Swapper

AppleJuice

Ares

Atomwire

AudioGalaxy

AudioGalaxy Satelite

AudioGnome

BadBlue
Bearshare
BlackWindow
Blipster Fast Find
BlubsterBoDeTella
BuddyShare
CatNap
Dagsta
DC++
DC:Pro
DietKazaa
DirectConnectDBNapster
Dopeflish Satellite
Earth Station
eDonkey Client
eDonkey Server Spy
eDonkeyboot Lite
eDonkey
ELF
eMule pHoeniX
eMule Plus
eMule
Evolution
Exware
ExoSee
FANtastic PLayer
File Freedom
Filemaze
FIlenavigator
FIlerouge
FIleShare Client
FIleSpree
Filetopia
Filetopia

FolderShare
Freewire
FTP++P2P
Gnutella
Gnotella
Gnucleus
Groskter
iMesh
Inoize
intelliMP3
Jungle Monkey
Kast
Kazaa Lite
Kazaa Kontrol Leech Killer
Kazaa Lite Advanced
Kaza Lite Cracked
Kazaa Cracked K++
Kaza Media Desktop
Kazearch
Kceasy
Limewire
Limewire Sparky
Locutus
IPhant
Madster
MediaSeek
Mercora
Mnet
Mojonation
Morpheus
MP3Mystic
MXlinx
MyNapster
Myster R8

NapAmp
Napigator
NapiMX
Napshack
Napster
Natural Born Chatter
Neo Modus Direct Connect
Neo Napster
Netbrilliant
NetMess
Newtella
NTella
Nudester
Nuzzly
OHAHA
OMNI
OpenCola
OpenNap
Overnet
PeerGenius
Phex
Phosphor
Piolet
Plebio
PornDigger
Private Peer to Peer
QtraxMax
QueerPeer
Rapigator
Razius Express
Renapster
RiffShare
RighteousMP3
Shareaza

ShareSniffer
SideKick
SlavaNap
Smirck
SongSpy XE
SoulSeek
SpookShare
Swapnut
Swaptor
Taxee
The Circle
The PornTrader
The Qube
ToadNode
TrustyFiles
URLBlaze
Varvar
VexTV
Wanafile
Wannafree
WinMX
Wippit
WWW Filre Share Pro
Xolox
Yaga Share
Yoink
Zalzah