Política Uso Aceptable de Recursos de TI

Pontificia Universidad Católica Madre y Maestra

Junio 2017

Política Uso Aceptable de Recursos de TI

Área: TI	Fecha: 1/06/2017
Información de Contacto: Francisco J. Sued	Referencia: **POL_TI_011_20100628**
Modificado por: Steven Sánchez	Versión: 2.0

Contenido

1. Introducción

1.1 Objetivo

El propósito de esta política es definir las pautas generales, para el uso de los sistemas, aplicaciones, redes y recursos informáticos que pertenezcan a la PUCMM.

1.2 Alcance

Esta política aplica a todos los empleados, estudiantes, consultores, auditores, contratistas o toda persona física o moral que aceda de forma directa o indirecta los recursos tecnológicos de la PUCMM, así como todas las transacciones electrónicas entre una o más partes de las antes mencionadas.

1.3 Glosario de Términos

*** Intranet:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet (TCP/IP). Puede tratarse de una red aislada, es decir no conectada a Internet.

*** Extranet:** Red que utiliza la tecnología de Internet para conectar la red local (LAN) de una organización con otra red externa.

*** Programas Maliciosos:** Se entiende como programas Maliciosos a los virus y otros programas dañinos.

*** Virus:** Se entiende por virus, un programa con la capacidad de reproducirse por medio de la modificación de otros archivos o programas.

*** Attachment:** Un archivo adjunto, archivo anexo, adjunto de correo. Es un archivo que se envía junto a un mensaje de correo electrónico. Pueden ser enviados no codificados o codificados.

*** Sniffer:** Programa y/o dispositivo que escucha los datos que viajan a través de una red.

*** Ping Flood:** Consiste en saturar una línea lenta con un número de paquetes ICMP suficientemente grande.

*** Packet Spoofing:** Técnica que consiste en hacer creer al receptor de un mensaje de correo electrónico que quien remite el mensaje es alguien de confianza.

*** Denial of Service (DoS):** Es un ataque de denegación de servicio, dirigido a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

*** Hacking:** Acción de piratear sistemas informáticos y redes de telecomunicación.

* Malware: es un programa o archivo creado con código malicioso, cuyo objetivo principal es causar daño a los sistemas de información.

* Adware: programa que extrae de manera no autorizada información personal a través de internet y reenvía la misma hacia otros sistemas. Esto es realizado a través del seguimiento de los hábitos de navegación de los usuarios con fines de presentar publicidad personalizada.

*** Cracking:** Es la modificación del software con la intención de remover los métodos de protección de los cuales éste disponga: protección de copias, versiones trial/demo, números de serie, claves de hardware, verificación de fechas, verificación de CD o molestias del software como pantallas irritantes y adware.

2. Políticas de Uso Aceptable de Recursos de TI

2.1 Uso General y Propiedad

2.1.1 Los recursos tecnológicos provistos por la PUCMM a sus empleados, tales como computadoras de escritorio, computadoras portátiles, tabletas, celulares, impresoras, teléfonos, entre otros, son para el ejercicio de sus funciones, por lo que los empleados deberán ejercer toda la debida prudencia y cuidado en la utilización de los mismos.

2.1.2 Toda información creada y/ó almacenada en los equipos y sistemas informáticos de la institución son propiedad de la PUCMM.

2.1.3 Los empleados son responsables de ejercer buen juicio respecto al uso personal de los recursos tecnológicos. Los usuarios deberán cumplir con el Código de Ética y Normativas para el uso de las Herramientas de Tecnología de la Información y Comunicación, así como también con el Documento de Responsabilidad y uso Adecuado de Equipos.

2.1.4 Los empleados de la PUCMM deben asegurarse que los equipos no atendidos, sean protegidos adecuadamente, incluyendo, pero no limitándose a:

a. Mantener las puertas cerradas donde alberguen equipos tecnológicos.
b. Realizar el cerrado de sesión (logoff) antes de dejar el computador desatendido.
c. Bloquear la estación de trabajo, para prevenir accesos no autorizados.

2.1.5 Acceso a material clasificado

Toda persona que acceda a los recursos de información de la PUCMM, está limitada al uso de la información al cual ha sido autorizada. Será sancionada cualquier persona a la cual se le encuentre o se le demuestre que accedió, leyó ó modificó información a la cual no ha sido explícitamente autorizada.

Toda información de carácter confidencial que sea transmitida fuera de la red interna de la PUCMM deberá ser debidamente protegida por los empleados que la manejen.

2.1.6 Por asuntos de seguridad y mantenimiento de la red, las personas autorizadas por la PUCMM, podrán monitorear los equipos, sistemas y tráfico de red en cualquier momento.

2.1.7 Todos los usuarios que opten por hacer uso de los recursos tecnológicos de la PUCMM, deberán firmar el Acuerdo de Uso Aceptable de Recursos Informáticos, así como también el Documento de Responsabilidad y uso Adecuado de Equipos. “Ver Acuerdo de Uso Aceptable de Recursos Informáticos”.

2.2 Seguridad de Información Propietaria

2.2.1 La PUCMM clasifica las informaciones contenidas en los sistemas relacionados al Internet, Intranet o Extranet, como confidencial o no confidencial. Todos los empleados deberán tomar las acciones necesarias, para prevenir el acceso no autorizado a las informaciones clasificadas como confidenciales. Ver documento "Clasificación de las información".

2.2.2 Todos los usuarios deberán mantener sus contraseñas aseguradas y no las compartirá con nadie. Los usuarios son los responsables de la seguridad de sus cuentas y contraseñas (users/passwords).

2.2.3 Las contraseñas de usuario tendrán un período de vigencia de noventa (**90**) días para los empleados administrativos y de (**180**) días para el personal Docente y Estudiantes, por lo que las contraseñas deberán ser cambiadas al final de este período. Será desplegado un aviso de advertencia indicando que la contraseña está a punto de expirar, a los quince (15) días previos de la fecha de expiración. "*Ver Política Manejo de Contraseña"*.

2.2.4 Todas las computadoras de escritorio y portátiles que estén enroladas al dominio administrativo o académico deberán ser aseguradas, con la utilización de protectores de pantalla (Screensavers) protegido por contraseña, que se activen automáticamente a los diez (10) minutos de inactividad. Además, estará deshabilitada la opción de modificación del Desktop para todos los usuarios administrativos. La excepción a esta política deberá ser tramitada a través de Recursos Humanos con su debida justificación.

2.2.5 Todas las computadoras de escritorio y portátiles de la institución tendrán una contraseña de administrador local, el cual sólo conocerá el personal responsable de la Unidad de Servicio al Cliente (USC) y la Unidad de Administración de Redes (UAR). Esta contraseña deberá ser cambiada cada **6** meses..

2.2.6 Todas las computadoras portátiles provista por la PUCMM al personal administrativo de la institución tendrán una contraseña de acceso al BIOS, el cual sólo conocerá el personal responsable de la Unidad de Servicio al Cliente (USC) y la Unidad de Administración de Redes (UAR). *Ver: "Política de Informática Móvil"*.

2.2.7 El personal de la Unidad de Servicio al Cliente (USC) deberá mantener configurado para todos los computadores propiedad de la institución con la secuencia de inicio del sistema operativo (Boot) por medio del disco duro.

2.2.8 Debido a que la información almacenada en las computadoras portátiles de la institución es especialmente vulnerable, se le debe prestar un cuidado especial.

Las computadoras personales deben estar protegidas de acuerdo con las "*Políticas de Informática Móvil"*.

2.2.9 Para minimizar la posibilidad de cualquier debilidad del sistema operativo, los usuarios administrativos con equipos propiedad de la Institución deberán conectar sus respectivas computadoras portátiles por lo menos una vez cada **15 días** a la red interna de la PUCMM, para que de esta manera se proceda a instalar automáticamente los parches del sistema operativo.

2.2.10 Se recomienda evitar el reenvío de correos de la institución a correos personales (Outlook (Hotmail), Yahoo, Gmail, etc.).

2.2.11 Se recomienda evitar el uso del correo de la institución para asuntos personales, por lo que se le debe advertir a sus contactos que no les envíen correos que no estén relacionados a su trabajo. Ver "Acuerdo de Uso Aceptable de Recursos Informáticos*"*.

2.2.12 No se debe registrar las direcciones de correo electrónico de la institución en sitios de Internet que no estén relacionados a las actividades de la institución.

2.3 Uso Inaceptable

2.3.1 La violación de los derechos de autor de cualquier persona o institución, violación de patente o cualquier otra propiedad intelectual, incluyendo, pero no limitando a la instalación y/o distribución de programas pirateados o cualquier otro programa o contenido que no esté propiamente licenciado por la PUCMM.

2.3.2 Se prohíbe que cualquier persona interna o externa a la institución utilice los recursos tecnológicos la PUCMM, para participar en actividades ilegales, ya sea esta local o foránea.

2.3.3 Se prohíbe compartir o revelar las contraseñas y/o permitir el uso de su cuenta de usuario a otras personas.

2.3.4 Queda prohibido el uso de los activos de la PUCMM para participar o promover propaganda política, acoso sexual, reventa o uso comercial del servicio, campañas electorales o cualquier uso ilegal, indebido o no autorizado por la institución que pueda provocar una acción judicial.

2.3.5 Se prohíbe almacenar, compartir o distribuir cualquier tipo de archivo digital mediante los recursos tecnológicos de la institución que violen las leyes sobre derecho de autor y propiedad intelectual, tales como archivos de video, audio, imágenes, entre otros.

2.3.6 No está permitido compartir discos o directorios en las computadoras locales de los usuarios con permisos de lectura y/o escritura, a menos que exista un

requerimiento justificado, debido a que esto puede provocar la propagación de virus informáticos en la red.

2.3.7 Queda prohibido compartir recursos y asignar permisos con la opción todo el mundo "**Everyone**".

2.3.8 Se prohíbe instalar en los equipos de la PUCMM programas P2P, los que se utilizan para bajar música, videos, programas u otros archivos.

2.3.9 Se prohíbe la instalación de juegos para fines recreativos en los equipos propiedad de la PUCMM.

2.4 Actividades del Sistema y de la Red

Las siguientes actividades, están estrictamente prohibidas sin excepción alguna:

2.4.1 Obtener acceso a través de las brechas de seguridad o interferir en el funcionamiento de la red de la PUCMM o de otras instituciones. El acceso a través de las brechas de seguridad incluye, pero no se limita al acceso de información que el empleado no está supuesto a acceder o que no es destinatario, utilizar un servidor o una cuenta la cual el empleado no esté expresamente autorizado a utilizar. Para los propósitos de esta sección, "interferir" incluye, pero no está limitado a, sniffing, ping floods, packet spoofing, denial of service, forget routing o cualquier otra técnica de intercepción, manipulación, phishing, hacking, cracking u otras manipulaciones maliciosas de información.

2.4.2 Las pruebas de tipo Port Scanning (escaneo de puertos), System Scanning (escaneo de sistemas) o cualquier monitoreo de la red están terminantemente prohibidas y sólo podrá ser ejecutadas por el personal autorizado de la PUCMM.

2.4.3 Evadir la autenticación de usuario o la seguridad de cualquier equipo, red o cuenta.

2.4.4 Interferir o denegar el servicio de cualquier equipo (Ej. Denial of Service Attack).

2.4.5 Usar cualquier programa/script/comando, o enviar mensajes de cualquier tipo, con la intención de interferir con, o deshabilitar, una conexión de usuario, por cualquier medio local o por vía de Internet/Intranet/Extranet.

2.4.6 Proveer información confidencial acerca de empleados o estudiantes de la PUCMM, a cualquier entidad ya sea interna o externa a la PUCMM de manera no autorizada.

2.5 Protección Contra Programas Maliciosos

2.5.1 Todas las computadoras y servidores propiedad de la institución y que se encuentren conectadas a la red interna de la PUCMM, deberán mantener sus respectivos programas antivirus actualizados a la última definición y deberán mantener las últimas actualizaciones de parches de seguridad a nivel del sistema operativo y las aplicaciones instaladas.

2.5.2 Queda prohibido la introducción de programas con códigos maliciosos a la red o a los servidores (Ej. Virus, Gusanos, Troyanos, Bombas de E-Mail, etc.) de la institución.

2.5.3 Los empleados deben ejercer extrema precaución cuando abran correos electrónicos con archivos adjuntos (attachments) que provengan de remitentes desconocidos, ya que pueden contener virus, programas troyanos o programas destructivos. En caso de recibir algún archivo adjunto con características sospechosas alusivas a este punto, el usuario deberá notificar de inmediato, a través del sistema de tickets de servicio o correo electrónico, a la Unidad de Servicio al Cliente o la Unidad de Administración de Redes.

2.5.4 Cualquier información que venga por medio electrónico o magnético como disquetes, CD, DVD, Discos Duros Externos, Memorias USB, correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser utilizada. Es conveniente que el usuario ejecute el software antivirus antes de utilizar cualquier dato de dichos dispositivos.

2.5.5 Es responsabilidad de los usuarios reportar, a través del sistema de tickets de servicios, correo electrónico o cualquier otro medio disponible, todos los incidentes de infección de virus a la Unidad de Servicio al Cliente (USC) o la Unidad de Administración de Redes (UAR).

2.5.6 Ningún usuario debe desarrollar, distribuir o introducir en el computador cualquier software que conozca o sospeche que tenga virus.

3. Responsabilidades

Todos los empleados de PUCMM tienen la responsabilidad de cumplir con esta política.

El personal de la Unidad de Servicio al Cliente (USC) y el personal de la Unidad de Administración de Redes (UAR) serán responsables de reportar a los empleados identificados que no cumplan con el compromiso de esta política.

La Unidad de Auditoría Interna debe determinar periódicamente el cumplimiento de las políticas.

4. Sanciones

El no cumplimiento de las disposiciones de esta política tendrá como consecuencia penalizaciones para la persona transgresora.

1) Primera vez amonestación escrita por la Dirección del área competente.
2) Segunda vez amonestación escrita por la Vicerrectoría de Administración y Finanzas (VAF).
3) Tercera vez despido justificado.

5. Historial de revisión

Este documento debe ser revisado y/o actualizado a partir de la fecha de su primera publicación e implementación por lo menos una vez al año.

Versión	Fecha de Revisión	Descripción de cambio	Preparado por	Autorizado por
1.1	05/01/12	Publicación original	Steven Sánchez	Alejandro J. Liz
1.2	03/03/14	Modificación	Comité Interno de TI	Alejandro J. Liz
2.0	1/6/2017	Modificación Derecho de Autor	Steven Sánchez	Francisco J. Sued

6. Anexo

A. Documento de ética y buenas prácticas para el uso de los sistemas de información.
B. Documento “Clasificación de la información”.
C. Acuerdo de Uso Aceptable de Recursos Informáticos.
D. Documento “Responsabilidad y uso adecuado de equipos”