NORMAS PARA EL MANEJO Y LA ADMINISTRACIÓN DE REDES AMPLIAS Y LOCALES

DOCUMENTO NORMATIVO I-1011-017

Introducción

Las redes de computadoras, tanto las amplias como las locales, prestan un servicio fundamental que permite a los usuarios interactuar con los recursos tecnológicos de la Universidad y del mundo exterior. Es de suma importancia que un recurso como éste se maneje de forma apropiada, asegurando su disponibilidad para que pueda utilizarse de forma flexible, pero segura, y sin poner en riesgo los sistemas de información de la Universidad.

I. Base legal

Estas normas se establecen en virtud de la autoridad conferida al Presidente de la Universidad por la Junta de Síndicos en los Estatutos de la Universidad y se apoyan en la política establecida por la Junta de Síndicos en el documento *Guías y Normas Institucionales para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones*; y en la *Reglamentación de la Universidad Interamericana de Puerto Rico sobre el Directorio de Estudiantes y Ex-Alumnos*.

Además, están en armonía con las leyes internacionales, federales y estatales aplicables que gobiernan la privacidad y confidencialidad de información, incluyendo el "Electronic Communications Privacy Act" de 1986, La Ley FERPA de 1974 (según enmendada), 20 U.S.C. 1232g y las regulaciones establecidas bajo, 34 C.F.R., Parte 99.

II. Propósito

Este documento tiene el propósito de establecer las normas para el control y administración de las redes amplias y locales de la Universidad.

III. Alcance

Estas normas aplican a las personas responsables del manejo y la administración de las redes de la Universidad.

Apartado 363255 • San Juan, Puerto Rico 00936-3255 • Tel. (787) 766-1912 • Fax (787) 751-3375

IV. Definiciones

Para propósitos de este documento, los siguientes términos tendrán el significado que se indica a continuación:

4.1 Área Restringida – lugar que debe tener un sistema de control de acceso.

4.2 Ataques informáticos – acción deliberada cuyo propósito es interrumpir la operación habitual de los sistemas de información o alteración de la información.

4.3 Bloqueadores de pantalla – mecanismo de seguridad mediante el cual el contenido de la pantalla de una computadora o terminal se hace invisible en la pantalla y sólo volverá a verse al entrar una contraseña.

4.4 Componentes de la Red – servidores, "firewall", enrutadores, equipo de acceso remoto, entre otros.

4.5 Ejecutivo principal – el Presidente, los Rectores y Decanos de las escuelas profesionales.

4.6 Enrutamiento – proceso de seleccionar la mejor ruta disponible para enviar datos a través de una red de información.

4.7 "Firewall" – sistema o grupo de sistemas que establece regulaciones comunes de seguridad para las redes privadas y la Internet, determinando a qué servicios de las redes pueden acceder los usuarios externos e internos.

4.8 Información sensitiva – toda información cuya develación al público general pueda afectar las operaciones de la Institución o de la comunidad universitaria.

4.9 Instalaciones de acceso remoto – cualquier instalación que no sea de la Universidad y que permita una conexión a una red.

4.10 Protocolos de las redes – reglas que se utilizan para establecer la comunicación entre los diferentes componentes de una red.

4.11 Puerto de servicio – representa el punto de referencia en el protocolo en donde se puede establecer una comunicación con una aplicación.

4.12 Segmento físico – agrupación de recursos de red que tengan una conexión en común en la misma topología de red.

4.13 Segmento lógico – agrupación lógica de los recursos de los equipos.

4.14 Servidor de autenticación central – servidor mediante el cual, de forma centralizada, se realiza la autenticación de los usuarios que se conectan a la red.

4.15 Unidad – la Oficina Central del Sistema, los recintos y las escuelas profesionales.

V. Normas generales

5.1 Las personas designadas para administrar las redes de la Universidad deberán estar debidamente adiestrados en las tecnologías sobre la seguridad y la administración de redes.

5.2 Las redes deberán estar diseñadas y configuradas para cumplir con las necesidades académicas y administrativas de la unidad.

5.3 Las redes deberán estar separadas en segmentos físicos o lógicos o ambos permitiendo el intercambio de datos entre las misma.

5.4 Las redes deberán poseer dispositivos o sistemas lógicos que las protejan contra el acceso no autorizado a recursos, información sensitiva y que las protejan de ataques informáticos internos y externos.

5.5 El acceso remoto a las redes se llevará a cabo mediante conexiones seguras que estén permitidas a los usuarios autorizados, según se define en el documento *Normas y Procedimientos de Servicios de Acceso Remoto.*

5.6 Cuando se vayan a realizar cambios o actualizaciones de seguridad en las redes, deberán llevarse a cabo de manera planificada y organizada, de forma que se evite cualquier impacto negativo en su funcionamiento.

5.7 Las personas responsables de administrar las redes realizarán monitoreo o inspecciones del tráfico en las redes, como parte de sus funciones normales, (ver Sección VII, Responsabilidades). Cuando no sean inspecciones de rutina solicitarán autorización del ejecutivo principal de la unidad o la persona que éste designe, salvo en los casos de circunstancias críticas, donde no actuar pudiera repercutir gravemente en el servicio general a la comunidad universitaria. En esos casos, el personal informará inmediatamente a su supervisor sobre el incidente y la acción tomada.

VI. Normas relacionadas con los componentes de las redes

6.1 Los servidores y otros componentes de las redes deberán estar físicamente localizados en un lugar con acceso controlado. El área deberá estar protegida por un dispositivo de seguridad seguro. Deberá tener un mecanismo de acceso para registrar quién entra y quién sale del área restringida.

6.2 El área restringida en la que los servidores y componentes de las redes estén ubicados, deberá mantenerse a una temperatura de ambiente controlado. Se recomienda que esta área tenga una fuente de energía independiente de la del resto del edificio.

6.3 La solicitud de acceso a las redes para facultad y administrativos, que requiera credenciales, tiene que documentarse por escrito utilizando el formulario Solicitud para Cuenta en la Red / Correo Electrónico, (ver Anejo).

6.4 Los puertos de servicios deberán estar controlados hasta que sean requeridos en producción.

6.5 Los servidores deben tener bloqueadores de pantallas con contraseña que desactivan el acceso a la consola del servidor automáticamente.

VII. Responsabilidades

7.1 Las personas responsables de administrar las redes de las unidades, tendrán las siguientes responsabilidades:

7.1.1 Determinar, procurar y mantener los componentes de la red necesarios para que las redes de la Universidad funcionen eficientemente.

7.1.2 Documentar los componentes de las redes incluyendo los accesos.

7.1.3 Monitorear el comportamiento, la seguridad y el tráfico de las redes.

7.1.4 Controlar los accesos a las redes, incluyendo las redes inalámbricas, de modo que se disponga de un nivel apropiado de seguridad virtual y física de los recursos.

7.1.5 Administrar los componentes de las redes como las direcciones IP, el enrutamiento de tráfico y los mecanismos de identificación de los recursos de las redes, entre otros.

7.1.6 Verificar periódicamente las bitácoras ("logs") y discutir los hallazgos con el Director de Informática y Telecomunicaciones de la unidad.

7.1.7 Documentar y actualizar el proceso de recuperación de desastres de la red.

VIII. Acciones disciplinarias

8.1 Cuando se determine que ha habido una violación a lo establecido en la *Guías y Normas Institucionales para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones* o lo dispuesto en este documento, se aplicarán las medidas correctivas y disciplinarias establecidas, de acuerdo con la gravedad de la infracción y conforme a las normas establecidas en los documentos oficiales.

8.2 Cuando el usuario no sea empleado regular de la Universidad, el Presidente o la persona que éste designe, recibirá el asesoramiento pertinente para determinar la acción a seguir.

IX. Separabilidad

Si cualquier parte o sección de estas normas es declarada nula por una autoridad competente, tal decisión no afectará las restantes.

X. Derogación o enmienda

Estas normas enmiendan el documento normativo I-0210-008R y cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto. Este documento puede ser enmendado o derogado por el Presidente de la Universidad.

XI. Vigencia

Estas normas tendrán vigencia inmediata a partir de la aprobación y firma del Presidente.

XII. Aprobación

Manuel J. Fernós
Presidente

4 de noviembre, 2011
Fecha (D-M-A)

Anejo: Solicitud para Acceder a la Red / Correo Electrónico

UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
CENTRO DE INFORMATICA Y TELECOMUNICACIONES

Solicitud para Acceder a la Red / Correo Electrónico

1. Fecha: _____

2 ☐ RED ☐ Email

3. ☐ Creación Cuenta ☐ Cancelación Cuenta ☐ Cuenta Temporera : ____/____/____

4. Indique al grupo que pertenece:

☐ Administración ☐ Facultad ☐ Otro: ☐

5. Nombre del Solicitante	
6. Número de Identificación	
7. Puesto	
8. Oficina	
9. Firma del Solicitante	
10. Nombre del Supervisor	
11. Firma del Supervisor	

☐ 12. La Universidad tiene disponible en su WEB SITE todos los documentos normativos, con los asuntos clasificados en dos categorías. Una para el uso público, la cual se accede a través de **http://documentos.inter.edu** y otra para uso de los empleados de la Universidad, bajo la categoría de restrictos, que se accede a través de ***Inter Web***. Me comprometo a cumplir con las Políticas, Normas y Procedimientos establecidos por la Universidad y por las Unidades.

MF

USO OFICIAL CENTRO DE INFORMATICA Y TELECOMUNICACIONES

1. Cuenta de usuario asignada:		2. Fecha comienzo:	
3. Fecha de expiración:		4. Fecha cancelación:	
5. Otorgado por:			
6. Contraseña inicial:		7. Correo electrónico asignado:	
8. Nombre Administrador(a) de la Red			
9. Firma Administrador(a) de la Red			

INSTRUCCIONES

1. Indique la fecha que completó la solicitud.
2. indique si aplica para la RED o Correo Electrónico (Email).
3. indique con una **X** si es creación de cuenta o Cancelación de cuenta en la RED o Correo Electrónico. Si la cuenta es temporera, indique hasta cuándo el usuario tendrá activa la cuenta.
4. Indique con una **X** al grupo que pertenece el solicitante: Administración, Facultad, CIT u Otros.
5. Indique el nombre del solicitante, al cual se le creará la cuenta.
6. Indique el número de Identificación del solicitante.
7. Indique el nombre del puesto del solicitante.
8. Indique el nombre de la oficina a la cual pertenece el solicitante.
9. Se requiere la firma del solicitante.
10. Indique (en letra de molde) el nombre del Supervisor del solicitante.
11. Se requiere la firma del Supervisor.
12. El solicitante tiene que indicar con una **X** su *compromiso de cumplir* con las *Políticas, Normas y Procedimientos* establecidos por la Universidad y las Unidades.

USO OFICIAL CENTRO DE INFORMATICA Y TELECOMUNICACIONES

1. Indique el USER NAME asignado.
2. Indique la fecha de creación de la cuenta.
3. Indique la fecha de expiración de la cuenta, hasta cuándo la cuenta estará activa. Aplica para usuarios temporeros.
4. Indique la fecha de cancelación de la cuenta.
5. Indique el nombre de la persona que otorgó la cuenta.
6. Indique la contraseña inicial.
7. Indique la dirección del correo electrónico asignado.
8. Indique (en letra de molde) el nombre del Administrador (a) de la Red.
9. Se requiere la firma del Administrador (a) de la Red.