NORMAS Y PROCEDIMIENTOS PARA LA PREVENCIÓN Y EL CONTROL DE ATAQUES INFORMÁTICOS

DOCUMENTO NORMATIVO I-0310-010R

Introducción

La Universidad Interamericana realiza una gran parte de sus tareas y servicios académicos y administrativos de forma electrónica. Por eso, las fallas que ocurren en los sistemas de información pueden crear situaciones en el ambiente de trabajo o estudios. Por otro lado, algunas personas crean aplicaciones con intenciones cada vez más dañinas. Consiguientemente, la Universidad deberá tener en sus normas una política apropiada para la protección de ataques informáticos en sus computadoras, de manera que pueda prevenir la entrada de virus y ataques que arriesgan la seguridad de las redes.

I. Base legal

Estas normas y procedimientos 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*; en las *Guías y Normas sobre derechos de Autor de la Universidad Interamericana de Puerto Rico*; y en la *Política Institucional de la UIPR sobre Directorio de Estudiantes y ex-Alumnos.* También, están en armonía con las leyes internacionales, federales y estatales aplicables que gobiernan la privacidad y la confidencialidad de información, incluyendo la Ley *Electronic Communications Privacy Act* de 1986, la Ley FERPA de 1974 (según enmendada), 20 U.S.C. 1232g y la regulación establecida bajo, 34 C.F.R., Parte 99, entre otras.

II. Propósito

Este documento tiene el propósito de establecer las normas y procedimientos para la prevención y control de ataques informáticos y mitigar su impacto en la red local de la Universidad.

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

III. Alcance

Estas normas y procedimientos aplican a todas las personas que tengan computadoras propiedad de la Universidad y tengan acceso a la red de la Universidad.

IV. Definiciones

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

4.1 Antivirus –programas que pueden detectar y eliminar virus informáticos, así como bloquear los virus para prevenir daño a los sistemas.

4.2 Ataque informático – evento o actividad que tiene por objeto alterar el funcionamiento normal de las computadoras, sin el conocimiento del usuario.

4.3 Comunidad universitaria – los miembros de la Junta de Síndicos, facultad, empleados no docentes, estudiantes y contratistas que ofrecen servicios a la Universidad.

4.4 Ejecutivo Principal - El Presidente de la Universidad, el Rector de cada Recinto, el Decano de la Facultad de Derecho y el Decano de la Escuela de Optometría.

4.5 "E-mail Gateway" – el portal existente entre la aplicación de correo electrónico y la Internet.

4.6 Junta de Síndicos – la Junta de Síndicos de la Universidad Interamericana de Puerto Rico, Inc.

4.7 Medidas antiataque – medidas para detectar y corregir ataques a los equipos y sistemas de información.

4.8 Presidente – el Presidente de la Universidad Interamericana de Puerto Rico, Inc.

4.9 Universidad o Institución – la Universidad Interamericana de Puerto Rico, Inc.

V. Normas

5.1 Toda computadora de la Universidad deberá tener instalada, una aplicación antivirus actualizada.

5.2 Como medida preventiva de ataque, ninguna computadora propiedad de

la Universidad o dispositivo móvil deberá conectarse a una red de la Universidad hasta que sean debidamente inspeccionados por el Centro de Informática y Telecomunicaciones de la unidad.

5.3 Cada "e-mail gateway" propiedad de la Universidad tendrá que utilizar un mecanismo de protección de ataques para el correo electrónico.

5.4 Los usuarios no cambiarán la frecuencia de la actualización automática de los programas antiataque, ni podrán interrumpir, desactivar o modificar las medidas antiataques.

5.5 Es necesario mantener informado a los usuarios de la Universidad del uso apropiado de los medios de protección provistos por la Universidad, así como asegurar que:

5.5.1 Se mantenga la integridad, confiabilidad y buen funcionamiento de los recursos de computación de la Universidad.

5.5.2 Los usuarios operen sus computadoras utilizando prácticas seguras.

5.5.3 Las aplicaciones y estrategias de protección de cada unidad funcionen eficientemente y se utilicen para los propósitos establecidos.

5.5.4 Se puedan prevenir o mitigar los ataques a los sistemas de información, en la medida que sea posible.

VI. Responsabilidades

6.1 Los directores de los Centros de Informática y Telecomunicaciones tendrán la responsabilidad de que, en su oficina, se lleven a cabo las siguientes funciones.

6.1.1 Procurar y mantener las medidas tecnológicas que se necesiten para que la Universidad pueda contar con las estrategias y recursos antiataques actualizados adecuados y efectivos en todos sus equipos.

6.1.2 Monitorear periódicamente el funcionamiento y la eficacia de las estrategias antiataques con el propósito de detectar posibles fallos en la operación.

6.1.2.1 Evaluar, según establecido por el Director de Informática y Telecomunicaciones los sistemas de información para detectar su posible vulnerabilidad.

6.1.3 Orientar a los empleados sobre la utilización de los recursos informáticos y cómo éstos pueden hacer vulnerable a la Universidad a ataques informáticos.

6.1.4 Mantener informada a la comunidad universitaria sobre las amenazas y tendencias que van surgiendo y cómo deberán actuar para prevenir problemas en sus equipos.

6.1.5 Tomar medidas para prevenir la perdida de información, datos y programas de las computadoras de la Universidad y reducir al mínimo el costo del mantenimiento y tiempo sin uso de la red, por la propagación de algún ataque.

6.2 Los Directores de Oficinas tendrán las siguientes responsabilidades.

6.2.1 Orientar al personal que utilice computadoras sobre las reglamentaciones de la Universidad con respecto al uso de sus recursos tecnológicos.

6.2.2 Asegurarse de que los empleados cumplan con lo establecido en las reglamentaciones de la Universidad.

6.2.3 Notificar al director del Centro de Informática y Telecomunicaciones de su unidad si observan los siguientes incidentes:

VII. Acciones disciplinarias

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 necesarias de acuerdo con la gravedad de la infracción y conforme a las normas establecidas en los documentos oficiales.

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

La violación a las normas por parte de un tercero autorizado podría dar lugar a la terminación de su contrato o asignación con la Universidad Interamericana.

VIII. Separabilidad

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

IX. Derogación o enmienda

Este documento enmienda el documento normativo I-0310-010 y deja sin efecto cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto y puede ser enmendado o derogado por el Presidente de la Universidad.

X. Vigencia

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

XI. Aprobación

Manuel J. Fernós, Lcdo.
Presidente

1/de noviembre, 2011
Fecha (D-M-A)