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

DOCUMENTO NORMATIVO I-0310-010

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 una crisis 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 las 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 sus 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 Universidad.

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

Se propone, además, asegurar que los usuarios de la Universidad estén enterados y acepten la responsabilidad del uso apropiado de los medios de protección provistos por la Universidad, así como asegurar que:

2.1 Se mantenga la integridad, confiabilidad y buen funcionamiento de los recursos de las computadoras de la Universidad.

2.2 Los usuarios operen sus computadoras utilizando prácticas seguras de computación.

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

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

III. Alcance

Estas normas y procedimientos aplican a toda persona que utilice computadoras en cualquier instalación física de la Universidad, que tenga acceso a la red de la Universidad o que utilice información a ser compartida con las computadoras de la Universidad mediante dispositivos móviles.

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 Dispositivos móviles –los *diskettes*, discos compactos, "pen drives" (*USB*), entre otros.

4.5 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.

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

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

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

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

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

V. Normas

5.1 Toda computadora de la Universidad deberá tener instalada, entre otras medidas antiataque, una aplicación antivirus, incluyendo las máquinas que no estén conectadas a una red.

5.2 Como medida preventiva de ataque, ninguna computadora 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 Todo servidor conectado a las redes de la Universidad tendrá que utilizar medidas antiataques, en consulta con el Centro de Informática y Telecomunicaciones de la Oficina Central del Sistema, incluyendo la configuración para detectar y eliminar los factores que puedan afectar los sistemas.

5.4 Cada "e-mail gateway" tendrá que utilizar un mecanismo de protección de ataques para el correo electrónico, aprobado por el director del centro de informática y telecomunicaciones de la unidad.

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

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, al menos una vez al mes, 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.

6.1.6 Evaluar periódicamente el número de incidentes de ataque para verificar si las normas establecidas mantienen su validez.

6.1.7 Crear un sistema de notificación automática e inmediata, una vez se haya detectado un ataque.

6.1.8 Cuando surja un ataque nuevo, notificar a los proveedores de servicio de antiataque para prevenir amenazas futuras.

6.1.9 Instalar las aplicaciones antiataques adquiridas por la Universidad cuando se le asigne una computadora a un empleado o, cuando se reprograme una máquina en uso.

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 de cualquier incidente reportado en 6.3.5.

6.3 Toda persona que utilice una computadora autorizada por la Universidad tendrá las siguientes responsabilidades.

6.3.1 Asegurarse de que su computadora tenga instalada la aplicación antiataque provista por la Universidad.

6.3.2 Mantener la aplicación de antiataque habilitada en su computadora todo el tiempo y con la configuración que le fuera provista por el director del centro de informática y telecomunicaciones de su unidad.

6.3.3 Si va a compartir información entre computadoras personales y las computadoras de la Universidad, mediante dispositivos móviles, utilizar una aplicación antiataque actualizada.

6.3.4 Realizar resguardos periódicos de la información en su computadora para recuperar eficientemente sus archivos, en caso de algún incidente.

6.3.5 Reportar a su supervisor inmediato, si observa:

6.3.5.1 que su computadora comienza a operar de forma errática.

6.3.5.2 que su computadora acumula cantidades anormales de correo electrónico o que los discos duros o dispositivos de almacenaje se llenan a capacidad con datos desconocidos.

6.3.5.3 que su computadora recibe mensajes con errores tipográficos, ya que esto puede indicar que se trata de un ataque.

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 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

13/3/10
Fecha (D-M-A)

ymc