Normas y Procedimientos de Acceso Remoto a la Red UIPR

(Documento Normativo 1-1011-018)

Introducción

En la Universidad Interamericana de Puerto Rico se ofrecen servicios académicos o administrativos de manera electrónica, los cuales requieren que algunos empleados o terceros se conecten remotamente a sus sistemas de información. La seguridad adecuada es la principal defensa que puede tener la Universidad al proveer sus servicios, ya que, de no tenerla, podría exponer su información privada y la estructura de la red a los posibles intrusos ("hackers") de Internet. Por eso, es importante que se evalúen y monitoreen adecuadamente los servicios que se proveerán por acceso remoto.

Todos los recursos y servicios de acceso remoto de la red se rigen por reglamentos institucionales, leyes federales e internacionales, según apliquen las mismas.

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 tienen su base en la política establecida por la Junta de Síndicos en los documentos Guías y Normas Institucionales para el Uso Apropiado de la Tecnología de Información, los Sistemas de Información Computadorizados y las Telecomunicaciones, en Reglamentación de la Universidad Interamericana de Puerto Rico sobre el Directorio de Estudiantes y Ex-Alumnos, en el Reglamento para la Administración de Documentos, en las Normas sobre la Confidencialidad de la Información, las Normas sobre Derechos de Autor de la Universidad Interamericana de Puerto Rico, en Procedimientos para la Divulgación de Información a Terceros, entre otros documentos normativos.

Estas normas y procedimientos se establecen, además, en armonía con las leyes internacionales, federales y estatales que gobiernan la privacidad y confidencialidad de la

información, incluyendo el "Electronic Communications Privacy Act" de 1986, la Ley FERPA de 1974 (según enmendado), 20 U.S.C. 1232g, y las regulaciones establecidas bajo 34 C.F.R., Parte 99, entre otras.

II. Propósito

El propósito de este documento normativo es establecer las normas y procedimientos que deberán seguirse para la seguridad en el servicio de acceso remoto. Se busca con esto proteger la información electrónica de la Universidad, la cual puede resultar inadvertidamente comprometida por los riesgos que implican las conexiones remotas a sus sistemas de información.

III. Alcance

Las normas y procedimientos aquí establecidos aplican a todo usuario autorizado por la Universidad.

IV. Definiciones

Para efectos de este documento los siguientes términos y expresiones tendrán el significado que se describe a continuación:

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

4.2. "Firewall" - sistema o grupo de sistemas que establece una política común de seguridad para red privada y la Internet, determinando a qué servicios de la red pueden acceder los usuarios internos y externos.

4.3. "Hacker" - persona con alto conocimiento técnico en la operación de computadoras, que podría violar la seguridad de las computadoras o redes electrónicas.

4.4. Junta de Síndicos - la Junta de Síndicos de la Universidad lnteramericana de Puerto Rico, lnc.

4.5. Presidente - el Presidente de la Universidad lnteramericana de Puerto Rico, lnc.

4.6. Protocolo TCP/IP - protocolo de comunicación utilizado para conectar redes a través de la Internet y otras redes de comunicación.

4.7. Universidad o Institución - la Universidad lnteramericana de Puerto Rico, lnc.

4.8. Usuario autorizado:

4.8.1 Personal de las unidades académicas que tiene una cuenta asignada en la red con el propósito de ejercer funciones laborales con autorización de acceso remoto.

4.8.2 Personal externo a la Universidad que requiere acceso remoto como parte de un servicio que provee a la Universidad.

4.9 VPN - red virtual privada que proporciona un medio para aprovechar un canal público como la Internet, para tener un canal privado o propio, que permita comunicar datos privados. Esto se logra con un método de codificación y un túnel seguro, que cree una vía privada y segura a través de la Internet.

Además, se adoptan las definiciones que apliquen, del documento Normas sobre la confidencialidad de la información.

V. Disposiciones generales

5.1. Toda persona que requiera conectarse remotamente a algún sistema de información deberá llenar la solicitud de acceso remoto para su debida autorización. El formulario de solicitud de acceso remoto se encuentra como anejo A de este documento.

5.2. Un empleado o usuario, a quien se le conceda el privilegio de acceso remoto, deberá estar consciente tanto de que la conexión entre su localidad y la Universidad son extensiones a la red de la Universidad, como de la responsabilidad que esto conlleva.

5.3. Toda conexión remota debe coordinarse con los centros de informática y telecomunicaciones.

5.4. Toda conexión remota a los servidores de la Universidad se hará mediante un método de conexión seguro con encriptación básica, como, por ejemplo, VPN.

5.5. Tanto los usuarios de la comunidad universitaria, como las personas externas a la Universidad a los cuales se le autorice el servicio de acceso remoto, deberán proteger los recursos de la Universidad en todo momento.

5.6. Todo permiso otorgado a conexión remota deberá eliminarse una vez finalice el trabajo autorizado.

VI. Responsabilidades

6.1. Los directores de los centros de informática y telecomunicaciones tendrán la responsabilidad de:

6.1.1 Implantar los procedimientos y mantener los recursos tecnológicos que se necesiten para que la Universidad pueda proveer los servicios de acceso remoto, basados en el servicio necesario o trabajo a realizarse, a los usuarios autorizados.

6.1.2 Ofrecer apoyo a las diferentes áreas que puedan requerir una conexión remota para que la misma pueda establecerse adecuadamente y de acuerdo con las normas de seguridad establecidas.

6.1.3 Evaluar alternativas costo-efectivas para establecer conexiones remotas seguras para que no pongan en riesgo los sistemas de información de la Universidad.

6.1.4 Recibir, evaluar y procesar las solicitudes de acceso remoto.

6.1.5 Hacer llegar el procedimiento aquí establecido al personal que pueda requerir conectarse al acceso remoto.

6.2. Los directores de cada oficina tendrán la responsabilidad de solicitar acceso remoto, utilizando la forma de Solicitud de Acceso Remoto, (Anejo). En la solicitud deberán justificar la necesidad del solicitante para que se le pueda proveer el acceso.

6.3. Los administradores de redes tendrán la responsabilidad de:

6.3.1 Configurar adecuadamente el "firewall" o cualquier otra aplicación, de modo que sólo los usuarios autorizados tengan acceso a los sistemas de la Universidad.

6.3.2 Monitorear la red de forma que se puedan detectar intentos de acceso no autorizados y se pueda identificar cualquier actividad inusual en los servicios de acceso remoto, como podrían ser los siguientes:

6.3.2.1 Múltiples conexiones de una misma cuenta activadas a la vez.

6.3.1 Tráfico inusual (sesiones de Telnet que no deberán existir, uso excesivo de ancho de banda y tráfico fuera de horas laborales) en la utilización de los servicios.

6.3.2.3 Violaciones a 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 otros documentos institucionales.

6.4. Todo usuario que requiera conectarse al acceso remoto tendrá la responsabilidad de:

6.4.1 Solicitar acceso remoto al director de la oficina correspondiente.

6.4.2 Hacer uso adecuado del recurso de acceso remoto de acuerdo con las políticas y regulaciones vigentes en la Universidad.

6.4.3 Asegurarse de que personas ajenas no utilicen dicha conexión para lograr acceso a los recursos informáticos de la Universidad

VII. Procedimientos

7.1. Los centros de informática y telecomunicaciones recibirán por correo electrónico la solicitud de servicios de acceso remoto.

7.2. Si la solicitud es para acceder a información de índole confidencial, se verificará que el usuario haya firmado un acuerdo de confidencialidad con la Universidad o que el acuerdo esté incluido en el contrato firmado con la Universidad. La cláusula del contrato se recoge en el documento normativo **Procedimientos para la Divulgación de Información a Terceros**.

7.3. Los directores de informática y telecomunicaciones determinarán si la solicitud procede y cumple con los requerimientos de estas normas y procedimientos. De proceder y cumplir con los requisitos, se otorgará el acceso o accesos solicitados.

7.3.1 Activación y terminación de cuentas.

7.3.1.1 El administrador de la red o su delegado abrirá la cuenta del usuario, una vez reciba la solicitud autorizada por los directores de los centros de informática y telecomunicaciones.

7.3.1.2 El administrador de la red notificará a la persona solicitante los códigos y claves de acceso correspondientes.

7.3.1.3 El administrador de la red desactivará la cuenta del usuario cuando los directores de los centros de informática y telecomunicaciones soliciten la desactivación, o cuando el administrador del servicio de autenticación detecte alguna actividad sospechosa en la cuenta que pueda estar violando las normas de la Institución.

7.4. Los directores de informática y telecomunicaciones o sus designados monitorearán el acceso provisto a los usuarios, siguiendo el proceso establecido por el Centro de Informática y Telecomunicaciones del nivel central.

VIII. Acciones disciplinarias

8.1. Cuando se determine que ha ocurrido 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 otros documentos institucionales, se aplicarán las medidas correctivas y disciplinarias necesarias de acuerdo con la gravedad de la infracción y en conformidad con las normas establecidas en los documentos oficiales.

8.2. 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 necesario para determinar la acción a seguir.

8.3. Las violaciones por parte de un tercero autorizado podrían dar lugar a la terminación de su contrato o asignación con la Universidad.

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 derogan el documento normativo l-0310-009R Normas y Procedimientos para la Seguridad en el Acceso Remoto a la Internet y otras Redes Electrónicas y cualesquiera otras directrices que estén en conflicto con lo aquí dispuesto y 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, Lcdo.
Presidente

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