Universidad de Puerto Rico en Bayamón
#170 Carr. 174 Parque Industrial Minillas
Bayamón, PR 00959
Tels. (787) 993-8853, (787) 993-0000, Ext. 3035 o 3037, Fax (787) 993-8900

Junta Administrativa
Secretaría

CERTIFICACIÓN NÚM. 43-2015-2016

Yo, Arnaldo Rodríguez Rivera, secretario ejecutivo de la Junta Administrativa de la Universidad de Puerto Rico en Bayamón, **CERTIFICO QUE**:

> La Junta Administrativa, en reunión ordinaria celebrada el 9 de febrero de 2016, luego de discutir el informe presentado por el *Comité de ley y reglamento*, aprobó la *Política para la interconexión y seguridad de la infraestructura de comunicación en la Universidad de Puerto Rico en Bayamón* que se incluye como parte de esta certificación. La *Política* entrará en vigor inmediatamente.

Y PARA QUE ASÍ CONSTE, expido la presente certificación en Bayamón, Puerto Rico, hoy 16 de febrero de 2016.

Arnaldo Rodríguez Rivera
Secretario Ejecutivo

Vo.Bo. Margarita Fernández Zavala
Rectora

POLÍTICA PARA LA INTERCONEXIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA DE COMUNICACIÓN EN LA UNIVERSIDAD DE PUERTO RICO EN BAYAMÓN

I. INTRODUCCIÓN

La Universidad de Puerto Rico en Bayamón (UPRB) ha establecido una infraestructura de comunicación que sirve de plataforma para la variedad de sistemas y servicios que tiene y ofrece. Estos están disponibles para el uso de la comunidad universitaria y son parte vital en las actividades académicas y administrativas.

Este documento establece las políticas institucionales para otorgar acceso, permitir conexión y garantizar la seguridad de la infraestructura de comunicación de la UPRB. Se identifican las responsabilidades de parte de la Oficina de Sistemas de Información (OSI) con la administración de la infraestructura y las responsabilidades de los usuarios. Además, se establece la facultad de OSI para tomar las medidas y las acciones necesarias para prevenir, detectar y corregir riesgos en la seguridad que amenacen la estabilidad y el funcionamiento de la red o interfieran con las actividades de la comunidad universitaria.

II. PROPÓSITO

El propósito de esta política es establecer la responsabilidad y la autoridad de OSI sobre la infraestructura de comunicación de la universidad, así como las responsabilidades correspondientes a los usuarios. Define, además, que la conexión de cualquier dispositivo o equipo debe ser aprobado previamente por OSI, pero siempre permitiendo y respetando la libertad de cátedra en la labor docente y de investigación.

III. RESPONSABILIDADES DE OSI

A. La OSI tiene a su cargo las tecnologías de información de la UPRB. Por consiguiente, esta oficina está facultada para manejar los aspectos de administración, de desarrollo, de instalación, de operación y de mantenimiento de la infraestructura de comunicación a favor de la comunidad universitaria (*Certificación 35-2007-2008 de la Junta de Síndicos*). Además, tendrá la tarea de divulgar esta política. Dentro de sus responsabilidades están:

1. Tomar las acciones necesarias para salvaguardar la seguridad y la confidencialidad de la data transmitida en la red.

2. Minimizar o detener riesgos potenciales a la infraestructura, a la UPRB o a sus miembros.

3. Referir a la autoridad nominadora los casos de violaciones a la seguridad o uso inadecuado de la infraestructura de comunicación institucional.

4. Garantizar la calidad del servicio brindado a todos los usuarios.

5. Planificar la expansión y la modernización de la infraestructura de comunicación.

6. Monitorear los equipos y el tráfico de data en la infraestructura de comunicación.

IV. ALCANCE

Esta política aplica a todos los miembros de la comunidad universitaria, personas externas que prestan servicios a la UPRB, así como cualquier usuario de los recursos de tecnologías de información y servicios de telecomunicación institucionales. También aplica a las facilidades de uso con equipo de computadoras, tales como: laboratorios de computadoras, salas, salones de clase, cuartos de servidores, gabinetes de redes o comunicación, equipos de conexión inalámbrica y centros de cómputos.

V. BASE LEGAL

A. Esta política se adopta a tenor con las siguientes disposiciones:

1. Ley Núm. 151 (2004), según enmendada — *Ley de Gobierno Electrónico*

2. Certificación 35-2007-2008, Junta de Síndicos de la UPR

3. *Procedimiento de la Oficina de Sistemas de Información de la administración central de la Universidad de Puerto Rico para utilizar y administrar la tecnología informática*

4. *Estándares para la utilización aceptable de recursos de tecnología informática* emitidos el 4 de abril de 2008 por la Vicepresidencia de Investigación y Tecnología de la administración central de la UPR.

5. *Políticas de tecnologías de información gubernamental* (TIG) establecidas por la Oficina de Gerencia y Presupuesto del Estado Libre Asociado de Puerto Rico

VI. DEFINICIONES

A. *Equipo*

Cualquier dispositivo, tales como computadoras, servidores, computadoras portátiles, tabletas, teléfonos inteligentes, copiadoras, faxes u otros que sea utilizado por un usuario y cuente con el acceso o capacidad de acceso a la infraestructura de comunicación.

B. *Equipo de comunicación*

Equipo o componente requerido para la conexión u operación de la red institucional, tales como: *switches, routers, firewalls, wireless access points, hubs* y otros.

C. *Usuarios*

Está facultada para hacer uso de la infraestructura de comunicación institucional toda persona registrada a través de solicitud de cuenta de acceso, de registro de equipo inalámbrico o permiso especial.

D. *Política de interconexión y seguridad*

Se refiere a la *Política para la interconexión y seguridad de la infraestructura de comunicación en la UPRB*.

E. *Punto de comunicaciones*

Lugar donde ubica la conexión principal del edificio o área a la infraestructura de comunicación, así como los espacios de distribución de las líneas de comunicación.

F. *Funcionario autorizado*

Empleado que ocupa un puesto de *especialista en equipo de computación y telecomunicaciones, técnico en tecnologías de información* u otro puesto relacionado (según el *Plan de clasificación y retribución del personal no docente la UPR*) que esté adscrito a OSI, o alguna otra oficina o departamento. Estos funcionarios

atienden las necesidades y los trabajos relacionados con los recursos de tecnologías de información en sus oficinas o departamentos en coordinación con OSI.

G. *Autoridad nominadora*

El rector o rectora es la autoridad nominadora en cada unidad, de acuerdo con lo establecido en la *sección 19.4–Autoridad de los rectores* del *Reglamento general de la UPR*.

VII. DISPOSICIONES GENERALES

A. Toda persona que utilice los servicios que ofrece la infraestructura de comunicación universitaria deberá conocer y cumplir con el reglamento vigente. Deberá registrarse con las credenciales otorgadas por OSI y con esto asume responsabilidad del uso de la infraestructura de comunicación de la UPRB. Esto aplica al uso del equipo de la institución, así como al equipo personal propiedad de los miembros de la comunidad universitaria (teléfonos inteligentes, tabletas y computadoras portátiles, entre otros).

B. La infraestructura de comunicación universitaria comprende el cableado de fibra óptica, cableado en cobre, enlaces inalámbricos, equipos de comunicación de datos y telefonía, enlaces de telecomunicaciones y programado necesario para su operación, distribuidos en sus edificios y predios del campus universitario.

C. La infraestructura de comunicación, los sistemas informáticos y servicios electrónicos serán utilizados para la docencia, la investigación y la gestión administrativa.

D. Cada punto de acceso a la red está diseñado para la conexión de una sola computadora o dispositivo, por lo que no se permite la conexión de equipos adicionales de comunicación o de computadoras con función similar a través de *switches, routers, firewalls, wireless access points* y *hubs*, entre otros.

E. No se permite el uso de mecanismos para la manipulación de direcciones de red que puedan afectar la topología o la estructura lógica de la red.

F. La instalación de puntos de distribución de acceso a la red se hará conforme a los criterios y a los estándares establecidos por OSI. Los trabajos correspondientes se harán en coordinación con OSI.

G. Se solicitará asesoramiento técnico de OSI para la adquisición de equipos de comunicación que se conectarán a la infraestructura institucional de manera que se contemplen los requisitos establecidos: calidad, compatibilidad, capacidad, garantías y servicios, entre otros.

H. Todo equipo de comunicación debe ser registrado junto con la información y datos de contacto del funcionario responsable del equipo. Para esto debe recibir una dirección IP y nombre (si aplica) asignados por OSI.

I. Se requiere mantener un registro actualizado que incluya: nombre de los servidores, sistema operativo, fecha de instalación, dirección de IP y descripción breve de su función principal. Este registro es responsabilidad del funcionario autorizado asignado a un departamento u oficina, quien deberá someter anualmente una copia a la OSI.

J. Los equipos de comunicación principales de la red serán instalados, configurados y mantenidos por OSI.

K. Ningún usuario estará autorizado a utilizar analizadores del tráfico que circula por la red o herramientas de rastreo de puertos que permitan detectar vulnerabilidades, excepto en el caso de los laboratorios instruccionales preparados especialmente para estos fines.

VIII. DISPOSICIONES ESPECÍFICAS

A. Seguridad física

1. Los puntos de comunicación deben ser contenidos en áreas seguras o controladas para protegerlas del acceso no autorizado, de daño físico o de interferencias. Las facilidades principales de comunicación deben quedar fuera de áreas de acceso público o directo. Los directorios de edificios o diagramas de localización no deben identificar la ubicación de las facilidades de comunicación.

2. Deben ser ubicados en áreas seguras con protección ambiental y control de acceso (piso a techo). Los requisitos de protección y ubicación se considerarán de acuerdo con el valor o la importancia de los activos (equipos o componentes) y los servicios que lo componen.

a. Protección ambiental

1) Se debe instalar detectores de humo, calor, agua, alarmas y extintores.

2) Este equipo debe verificarse periódicamente, según las recomendaciones del fabricante.

b. Control de acceso

1) Se debe registrar los datos de visita (nombre, fecha, hora, razón) de personal no autorizado. Además, debe ser supervisado por personal autorizado del área.

2) Se le eliminarán inmediatamente los derechos de acceso (llaves y códigos de acceso electrónico, entre otros) un empleado que renuncie a su puesto o que cambie de funciones que no requiera el acceso a áreas seguras.

3) Se deben establecer medidas para garantizar la confidencialidad, la integridad y la protección contra robo de los equipos. Cuando estos se reciban para ser instalados posteriormente, se deberá almacenar en áreas seguras.

4) En aquellas áreas que no haya cuartos de comunicación designados, se utilizará un gabinete para ubicar los equipos de comunicación.

5) La planificación para nuevos edificios o instalaciones debe incluir los requisitos para las facilidades de infraestructura de comunicación, preferiblemente desde el proceso del diseño. Esta evaluación debe considerar demanda futura y capacidad de crecimiento de las facilidades.

B. Seguridad del equipo de comunicación

1. Los equipos de comunicación que componen la infraestructura de comunicación institucional deben contar con protección en caso de fallas eléctricas. Las instalaciones eléctricas provistas para los equipos deben cumplir con las especificaciones del fabricante. Aquellas facilidades de comunicación que sean de uso crítico deben contar con una fuente de energía ininterrumpida (UPS) o, de ser necesario, un generador. Estos equipos deben verificarse periódicamente de acuerdo con las recomendaciones del fabricante.

2. EI cableado horizontal o de líneas principales deben estar protegidos contra su interceptación, daños accidentales o maliciosos. Las líneas

principales (fibra óptica, *tie cables*, UTP) de comunicación deben ser instaladas en conductos de protección. En el caso de líneas principales de interconexión (exteriores), la instalación debe ser soterrada y con los conductos de protección requeridos por los estándares.

3. El equipo de comunicación debe recibir el servicio, mantenimiento y actualizaciones necesarias para asegurar su funcionamiento e integridad. El equipo debe recibir periódicamente el mantenimiento o actualizaciones recomendadas por el fabricante. El personal autorizado es el único que debe realizar el mantenimiento, el servicio o la reparación de estos equipos.

C. Conexión del equipo

1. El personal técnico de OSI o los funcionarios autorizados son los únicos que podrán instalar y configurar los equipos de comunicación y conectarlo a la infraestructura institucional.

2. Los equipos que sean utilizados para la labor docente o la investigación podrán ser instalados, configurados y conectados por los miembros de la facultad a cargo de dichas tareas o por los funcionarios autorizados. También podrá hacer esta tarea los estudiantes autorizados que estén bajo la supervisión de los empleados o funcionarios mencionados anteriormente.

3. La OSI puede desconectar cualquier equipo que determine que afecta o compromete el funcionamiento de la red institucional, sin previa notificación a la persona u oficina responsable del mismo.

4. La OSI puede denegar la conexión de equipo de comunicación que no cumpla con los requisitos y estándares institucionales establecidos.

5. La OSI tendrá la facultad para realizar procesos de monitoreo de la infraestructura institucional y de recopilación de información para su análisis. Esto incluye, entre otros, el tráfico en la red interna de UPRB hasta el punto de enlace con la Administración Central.

D. Usuarios de la infraestructura de comunicación institucional

1. Todos los usuarios de la red de UPRB deben cumplir con las responsabilidades y obligaciones establecidas:

a. Solicitar o renovar su registro o cuenta de acceso a través del procedimiento establecido por OSI.

b. Cumplir con las políticas, los procedimientos institucionales, los reglamentos y las leyes, tanto estatales como federales, que apliquen al uso de los recursos de tecnologías de información.

c. Notificar a OSI o al funcionario autorizado correspondiente, cuando exista problemas con la conexión a la red o con el equipo.

d. Solicitar a OSI asesoría para la adquisición, la actualización o el cambio de equipo de comunicación.

e. Coordinar y asesorarse con OSI para la instalación, la modificación o la ampliación de las facilidades de conexión de acceso (*drops*), además de la supervisión de estos trabajos.

2. Las siguientes prohibiciones aplican a todos los usuarios de la infraestructura institucional:

a. Utilizar la infraestructura de comunicación, los recursos o los servicios con fines distintos a los académicos, de investigación o de administrativos de la institución, así como emplear los recursos o las facilidades con fines comerciales o lucrativos.

b. Usar la infraestructura universitaria para ganar acceso no autorizado de otros sistemas, ya sean locales o remotos.

c. Asignar direcciones IP sin autorización previa de OSI.

d. Facilitar, prestar o permitir el uso de la conexión de acceso o el equipo a personas no autorizadas.

e. Instalar, conectar o implementar equipos o sistemas que afecten, comprometan o interrumpan el funcionamiento de la red, los usuarios u otros sistemas.

f. Conectar, apagar o desconectar el equipo principal de la infraestructura institucional.

g. Utilizar direcciones de IP de la UPRB para configurar o conectar equipo no autorizado o ajeno a la institución.

IX. ACCIONES CORRECTIVAS

A. La OSI puede investigar, detener y resolver problemas o fallas en la seguridad de la infraestructura de comunicación universitaria. Para realizar esta labor, está facultada para desconectar, bloquear o recopilar (*log*) la información de cualquier equipo que utilice o tenga conexión con esta infraestructura. La OSI podrá tomar las siguientes acciones correctivas cautelares:

1. Suspender la cuenta de acceso o desconexión del equipo hasta resolver la situación.

2. Suspender temporeramente el acceso a la infraestructura de comunicación universitaria.

3. Notificar o referir a la autoridad nominadora a usuarios que abusen o no cumplan con esta política para las acciones disciplinarias correspondientes, según se establecen en el *Reglamento general de la UPR* y en el *Reglamento general de estudiantes.*

X. VIGENCIA

Esta política entrará en vigor el 9 de febrero de 2016.