# Normas y Procedimientos para el Desarrollo y Mantenimiento de la Infraestructura Tecnológica

Número: RRP-2017-004

Fecha: 14-08-2017

Autoridad Nominadora:

Dr. Luis A. Ferrao Delgado
Rector Interino

Oficina Responsable: División de Tecnologías Académicas y Administrativas

# TABLA DE CONTENIDO

# INTRODUCCIÓN

La División de Tecnologías Académicas y Administrativas (en adelante DTAA), unidad adscrita a Rectoría del Recinto de Río Piedras de la Universidad de Puerto Rico, tiene a su cargo los sistemas de información que se utilizan en los diferentes procesos administrativos y académicos, tales como: el Sistema Estudiantil, servicios de cuentas "*wireless*" y de educación a distancia, entre otros.

En la DTAA, la Sección de Infraestructura y Redes (Networking) es la encargada de las telecomunicaciones y servicios esenciales para que las comunicaciones dentro y fuera del Recinto trabajen de forma óptima. Entre sus áreas de trabajo están las siguientes:

- Redes Inalámbricas
- Redes Cableadas
- Equipos de Telecomunicaciones
- Servidores y sus Sistemas Operativos
- Seguridad a todas las áreas antes mencionadas

El impacto que tienen estas áreas con el Recinto es considerado crítico por su estrecha relación con la infraestructura tecnológica. Es por esta razón que se ha creado el documento de "*Normas y Procedimientos para el Desarrollo y Mantenimiento de la Infraestructura Tecnológica"*.

Este documento podrá ser revisado y/o actualizado anualmente, de ser necesario, para atender situaciones que pueden afectar el mismo tales como cambios en la estructura organizacional, en tecnología, equipos, programas, en las recomendaciones del fabricante, mejores prácticas, así como por cambios en procedimientos, normas o políticas institucionales, entre otras

**Unidad Responsable**
DTAA

**Otras Unidad(es) Concernida(s)**
N/A

**Puedo conseguir copia en**
DTAA

**Fecha de Efectividad:**
24/abril/2017

# I. PROPÓSITO

El propósito de este documento es el de establecer las normas y procedimientos uniformes a seguir por el personal de la Sección de Infraestructura y Redes de la División de Tecnologías Académicas y Administrativas (DTAA) del Recinto, con respecto a los sistemas de infraestructura que están bajo su control.

Este documento será una guía de trabajo para el personal de la Sección de Infraestructura y Redes de modo que puedan orientar y asegurarse de que los usuarios, personal técnico, administradores del Recinto fuera de la DTAA y terceros tales como contratistas, suplidores externos, consultores o visitantes, que se relacionen de alguna manera con la infraestructura, cumplan con las normas, parámetros operacionales, instalaciones y configuraciones establecidas por la DTAA en cumplimiento a los estándares mínimos de seguridad y de tecnología de dicha área.

# II. INTERPRETACIÓN Y DEFINICIONES

| | |
|---|---|
| **Access Point (Punto de acceso inalámbrico)** | WAP o AP por sus siglas en inglés: Wireless Access Point, es un dispositivo que permite conectar dispositivos que poseen una tarjeta de comunicación inalámbrica a la red. |
| **ANSI** | American National Standards Institute |
| **DHCP** | Dynamic Host Configurator Protocol - Protocolo de redes de computadoras y equipo para la configuración dinámica de los atributos de un equipo. |
| **DTAA** | División de Tecnologías Académicas y Administrativas |
| **EIA** | Electronic Industry Association - Organizaciones que establecieron y mantienen los estándares de la industria de cableado de telecomunicaciones. |
| **Firewall (Cortafuegos)** | Dispositivo que funciona como barrera entre redes, permitiendo o denegando la transmisión de paquetes de una red a la otra. |
| **Hardware** | Parte física de la infraestructura. |
| **Hub (Concentrador)** | Equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás. Similar al Switch (Conmutador), con la diferencia de que este corre a una velocidad fija (ejemplo: 10Mbps, 100Mbps, etc.) |

| | |
|---|---|
| **Mac Address (La dirección MAC)** | Media Access Control address o dirección de control de acceso al medio, es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. |
| **Red Inalámbrica** | Redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables. |
| **Router (Enrutador)** | Dispositivo para interconexión de redes de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. |
| **SNMP** | Simple Network Management Protocol - Protocolo de redes de computadoras y equipos que permite la administración remota simple de los equipos. |
| **Switch (Conmutador)** | Dispositivo de lógica de interconexión de redes de computadoras que opera en la capa dos (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los equipo en la red. |
| **TCP** | Transmission Control Protocol - protocolo de comunicación de redes de computadoras y equipos utilizados para la transmisión de datos. |
| **TIA** | Telecommunications Industry Association |
| **UDP** | User Datagram Protocol - Protocolo de comunicación de redes de computadoras y equipos utilizados para la transmisión de datos. |

# III. ALCANCE

Este es un procedimiento interno que aplica a los administradores y personal técnico de la Sección de Infraestructura y Redes de la DTAA. En el documento se definen y establecen los parámetros para los procesos operacionales de administración, instalación, configuración y mantenimiento de la infraestructura que están bajo el control de la DTAA del Recinto de Río Piedras de la Universidad de Puerto Rico.

# IV. RESPONSABILIDADES

| | |
|---|---|
| **Director Ejecutivo** | 1. Corroborar que el personal de la Sección de Infraestructura y Redes cumpla con las funciones de monitoreo y control de la red del Recinto de tal forma que la misma se encuentre operante y segura.<br>2. Apoyar al personal en el uso de las nuevas y/o actuales tecnologías para que los sistemas y red del Recinto se mantengan en buen estado, con las medidas de seguridad requeridas y con el personal debidamente adiestrado. |
| **Director de la Sección de Infraestructura y Redes** | 1. Supervisar que el personal de la Sección de Infraestructura y Redes cumpla con lo establecido en este documento.<br>2. Procurar que se monitoree la red y se tomen las medidas de seguridad requeridas para mantener en forma segura y operante la red del Recinto. |
| **Personal de la Sección de Infraestructura y Redes** | 1. Estar al día sobre las regulaciones y estándares de las agencias reguladoras de comunicaciones y velar por que se cumplan con los mismos.<br>2. No permitir la conexión de equipos con nombres o direcciones no registrados. Orientar al usuario para que cuando un equipo deja de usarse, lo notifique a la DTAA- Infraestructura, para desconectar el mismo de la red y/o registrar los cambios.<br>3. Verificar que todos los equipos que los usuarios del Recinto deseen conectar a la red cumplan por lo menos con el mínimo de configuración de seguridad requerido por la DTAA.<br>4. Monitorear diariamente el tráfico de la red del Recinto para identificar posibles anomalías en el flujo regular y tomar las acciones pertinentes para normalizar la red.<br>5. Monitorear los equipos de comunicaciones que forman parte de la red, para verificar que estén activos y de haber alguno en estado inoperante, proceder con la revisión física en el lugar donde esté ubicado el mismo. |
| **Especialista en Tecnología de Computación II** | 1. Este puesto en específico monitorear el desarrollo de las tecnologías de redes, evaluar mejoras y si es apropiado incorporarlas para mejorar el rendimiento, capacidad, disponibilidad, seguridad y confiabilidad de la red.<br>2. Además, realiza todas las tareas descritas bajo “Personal de la Sección de Infraestructura y Redes. |

# V. PROCEDIMIENTO

## A. Normas Establecidas

La infraestructura que mantiene la DTAA está constituida por los equipos tecnológicos necesarios para dar apoyo a las operaciones del Recinto de Río Piedras de la Universidad de Puerto Rico, entre estos:

- Cableado de fibra óptica y el cableado de cobre que conforman la red de la Universidad.
- *"Routers y Switches"*
- Puertos de accesos inalámbricos
- Servidores
- Sistemas y equipos de resguardos
- Computadoras portátiles y de escritorio

Los sistemas informáticos, incluida su red de comunicaciones, están al servicio del cumplimiento de los fines propios de la Universidad en los ámbitos de la investigación, la docencia y la administración. Solamente podrán utilizar los recursos de sistemas aquellos usuarios o grupos de usuarios que estén expresamente autorizados.

## B. Funciones Relacionadas al Mantenimiento de la Infraestructura y Redes

Las principales funciones del personal con relación al mantenimiento de infraestructura y redes se describen a continuación:

1. Supervisión de instalaciones de cableado de fibra óptica y de cobre, equipos y programas necesarios para las distintas áreas y administración de los recursos de la red tales como equipos, "*switches"*, enlaces inalámbricos entre otros.
2. Registrar y asignar las cuentas de los usuarios que utilicen alguno de los servidores administrados.
3. Ayudar a los usuarios a resolver los problemas que surjan en el uso de las redes relacionados con los aspectos de seguridad, asignación de cuentas y de derechos de acceso a aplicaciones y servicios.
4. Coordinar la configuración, instalación, manejo y administración de los sistemas de telecomunicaciones y mantener el acceso de los usuarios registrado y autorizado.
5. Elaborar y monitorear los informes sobre el uso de la red, así como los históricos.

6. Monitorear el uso de la red, su rendimiento y sobre todo la seguridad con el fin de detectar posibles anomalías, ya sean debido a problemas por fallas normales en los equipos, por fallas provocadas o accesos no autorizados, entre otros.
7. Estar al día de las nuevas tecnologías en el campo de las redes y las telecomunicaciones que surjan en el mercado y evaluar su posible utilización.
8. Sugerir, organizar y capacitar a los usuarios sobre el uso de las redes, aplicaciones, servicios disponibles y en el manejo de equipos que los administradores del control de la red consideren necesarios.
9. Proveer asistencia, orientación y recomendaciones sobre el equipo de comunicaciones inalámbricas que se debe utilizar en la Universidad.
10. Aprobación e instalación de equipo y programas para la red inalámbrica del Recinto.

# C. Monitoreo y Control del Tráfico en la Red

Las reglas que aplican al monitoreo y control del tráfico en la red serán las siguientes:

1. Los equipos que se conectan a la red utilizarán una dirección IP asignada por el personal de la Sección de Infraestructura y/o Redes de la DTAA. Además, se configurará con la información de identidad y los datos del personal responsable del equipo.
2. No estará permitida la conexión de equipos con nombres o direcciones no registrados. El personal de infraestructura y redes deberá orientar al usuario con relación a que, si un equipo deja de usarse, deberá notificarse a la DTAA para desconectarlo de la red y/o registrar los cambios.
3. Todo equipo adquirido por los usuarios del Recinto y que requiera conectarse a la red deberá cumplir una configuración mínima de seguridad.
4. Ningún usuario estará autorizado a utilizar analizadores de tráfico en la red de la Universidad. Igualmente estará prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo las circunstancias que lo justifiquen.
5. No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar la topología o la estructura lógica de la red.
6. Sólo podrá conectarse físicamente a la red los equipos de comunicaciones que hayan sido autorizados por la DTAA.
7. El tráfico y paquetes a través de los "*routers"* y "*switches"* se monitoreará diariamente utilizando herramientas que permitan identificar anomalías en el flujo regular. Una vez se reconoce el tráfico inusual en la red, la persona encargada del monitoreo identificará el equipo que lo está generando y lo comunicará por escrito ya sea

mediante correo electrónico al Coordinador de Servicios Técnicos al Usuario y/o administrador del área al cual pertenece el equipo o al "*Help Desk*".

8. Se documentará la revisión de los resultados obtenidos con la herramienta de escaneo designada, actualmente "Nessus", de tal forma que quede como evidencia las acciones tomadas. Se deberá documentar quedando como evidencia el análisis de su contenido, las medidas correctivas en los casos que aplique y la notificación al administrador de los equipos afectados que no estén en control de la DTAA.
9. Se monitoreará los equipos de comunicaciones que forman parte de la red para determinar que están activos. En el caso de que se identifiquen equipos en estado inoperante, el personal de la oficina deberá visitar el lugar para hacer una revisión física.
10. Se podrá identificar la siguiente información de los recursos conectados a la red: Dirección IP, Tráfico (TCP/UDP) origen/destino, Aplicaciones
11. De ser necesario se asignará prioridad del uso de ancho de banda conforme a los usuarios de una aplicación, un grupo de redes o subredes IP. Esta prioridad de tráfico se establecerá de acuerdo a la naturaleza e importancia del servicio.
12. Se mantendrán estadísticas de rendimiento de la red y de los servidores, que sirvan para medir la eficiencia de la red (tráfico TCP retransmitido), la cantidad de TCP experimentado, cantidad de conexiones TCP ignoradas, conexiones abortadas, retardo transaccional total, para aplicaciones transaccionales como: HTTP, Mail, Oracle, etc.
13. Se vigilará que los usuarios no pongan en riesgo la seguridad de la red universitaria, ya sea por vandalismo a la infraestructura y/o por utilización de programas que permitan alterar la integridad de los dispositivos conectados a la red.
14. El equipo de comunicaciones estará colocado en espacios asignados con acceso limitado al personal autorizado. La Sección de Infraestructura y Redes será responsable del control del acceso de los cuartos de comunicaciones. Para más información referirse al documento de "*Procedimiento de Custodia y Control de Llaves de Cuartos de Comunicación y Cableado" de la DTAA.*
15. Se mantendrá un diagrama en el que se contemple la ubicación y las diferentes conexiones de los elementos de la red incluyendo aquellos que se refieran especialmente a la seguridad (servidores, "*routers"*, "*firewalls"*, etc.). Cada vez que se realice un cambio, ya sea de adición, remoción, movimiento de equipo o cuartos de comunicación, deberá actualizarse el diagrama.
16. Las áreas que necesiten desconectar equipo(s) como parte de una remodelación, deberán dar aviso, preferiblemente por escrito a la DTAA con varios días laborables de anticipación, para tomar las medidas preventivas correspondientes, ya que los equipos instalados a través de la Universidad no deberán ser manipulados o reubicados sin autorización.
17. Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones de la Universidad podrá ser desconectado y se le notificará al usuario para la acción

correspondiente. También se le notificará al Director de la DTAA o su representante autorizado.

# D. Reglamentaciones y Estándares

Se deberán considerar los reglamentos y estándares vigentes. A continuación, se detallan los reglamentos y estándares actuales aplicables para trabajos a realizarse que impacte el área de comunicaciones en el Recinto:

1. Todo equipo a ser utilizado en la red inalámbrica debe cumplir como mínimo con el estándar 802.11g de comunicación inalámbrica.
2. Todo equipo debe cumplir con todas las reglas de las agencias reguladoras de comunicaciones, tales como la *Federal Comunications Commission* (FCC) y las políticas de la Universidad.
3. Todo contratista, consultor o compañía externa que realice instalaciones de trabajos relacionados al área de comunicaciones deberá cumplir con las siguientes guías:
   - Cumplir con los estándares vigentes de la ANSI/TIA/EIA:
     - ANSI/TIA/EIA-568 (todas sus partes) *Telecommunication Cabling Standard*
     - ANSI/TIA/EIA-569 (todas sus partes) *Standard For Telecommunication Pathways and Spaces*
     - ANSI/TIA/EIA-606 *Administration Standard for the Telecommunications Infrastructure*
     - ANSI/TIA/EIA-607 Generic Telecommunication *Bonding and Grounding (Earthing) for Customer Premise*

# E. Normas para la Red Inalámbrica

La Sección de Infraestructura y Redes deberán seguir las normas establecidas para la red inalámbrica, las cuales son las siguientes:

1. Las comunicaciones inalámbricas no proveen codificación de los datos transmitidos. La protección de los datos es responsabilidad del usuario y de la aplicación que se utilice para transmitirlos.
2. El equipo estará protegido con medidas de seguridad para prevenir el hurto o acceso no autorizado.
3. Toda compra de puntos de acceso en el Recinto, deberá ser consultada con el personal técnico del área de infraestructura y redes de la DTAA para asegurarse de cumplir con las especificaciones requeridas de compatibilidad de la red de comunicaciones del Recinto. No se permitirá la instalación de los mismos con conexión a la red si previamente no ha sido autorizado por el personal de infraestructura, y toda compra deberá ser autorizada por la DTAA, cuando proceda.

4. Los equipos de la red inalámbrica deberán ser instalados, configurados y administrados por el personal técnico de infraestructura o redes de la DTAA.
5. Para que un usuario tenga acceso a la red inalámbrica este debe tener la información de cuenta de empleado o estudiante. En caso que sea un equipo que no soporte autenticación (ej. Televisores) el acceso se otorgará basándose en *el MAC Address*. Para esto se hará una cuenta en el *Active Directory* utilizando el *MAC Address* como usuario y contraseña.

# F. Uso del Firewall

Las normas definidas para el uso del Firewall se encuentran en el manual de "**N*ormas y Procedimientos para la Configuración Básica de Servidores y Control de Acceso a través del Firewall*"** de la DTAA**.**

# G. Red Inalámbrica

El propósito de la red inalámbrica es proveer a la comunidad universitaria y visitantes conexión a sus dispositivos personales e institucionales que tengan asignados.

## 1. Nombre del servicio

Entre los servicios autorizados a ofrecerse a través de las redes inalámbricas están los siguientes:

| Nombre del Servicio | Puerto del Servicio | Descripción |
|---|---|---|
| http | 80 | Servicio de páginas de Internet |
| https | 443 | Servicio de páginas de Internet método seguro |
| Secureshell (ssh) | 22 | Conexión segura para acceso remoto |
| Telnet | 23 | Conexión no-segura para acceso remoto |
| SMTP | 25 | Servicio de envío de correo electrónico |
| IMAP | 143 | Servicio de correo electrónico |
| POP3 | 110 | Servicio para recibir correos electrónicos |

## 2. Equipo

| Nombre de Equipo | Descripción |
|---|---|
| Wireless-Nat | Equipo encargado de traducir direcciones privadas a las públicas del Recinto. |

| | |
|---|---|
| Wireless-Radius | Equipo encargado de otorgar autorización a clientes y puntos de acceso. |
| Wireless Access Points | Equipos que se distribuyen en el Recinto para otorgar acceso inalámbrico. |
| Wireless-Controller | Equipo responsable del control de los puntos de acceso y provee la configuración necesaria para el funcionamiento de la red inalámbrica. |

## 3. Pruebas de Campo

El personal de la Oficina tiene la responsabilidad de hacer un estudio de la dispersión de la señal y de localizar efectivamente los puntos de acceso previo a la instalación del mismo. Para este estudio de campo se utilizan varios *Access Point* (AP) y las herramientas de pc para medir la potencia de la señal. El estudio se realiza de la siguiente manera: se posiciona el *Access Point* (AP) en el lugar propuesto y se mide la calidad de la señal. Una vez la señal mida menos de cincuenta por ciento (50%) se debe posicionar otro AP para garantizar la calidad de señal. La señal se garantiza cuando se seleccionan diferentes canales para cada AP para de esta forma evitar la interferencia y obtener mejor rendimiento de la red inalámbrica.

## 4. Configuración

El *Access Point* (AP) como parte de su configuración, se conecta en el *switch* más cercano al área donde se interesa cubrir y se asigna el puerto al VLAN de AP's asignado . Se espera que el servidor de DHCP (*Dynamic Host Control Protocol*) le asigne un número de IP (*Protocolo de Internet*). Todos los AP deben tener la imagen "*light weight*", de esta manera los parámetros de configuración y redes serán provistos por el controlador.

Controladores nuevos se añadirán como clientes a la base de datos del RADIUS (*Remote Access Dial-In User Server*). El RADIUS es utilizado para autenticar clientes inalámbricos utilizando la cuenta de empleado ó estudiante configurada en el *Active Directory*.

## 5. Instalación

La instalación de los puntos de acceso la realiza el personal de infraestructura de la DTAA. El personal tiene todas las herramientas y equipos necesarios para llevar a cabo dicha instalación la cual se hará preferiblemente en una oficina a la que sólo tendrán acceso los empleados. Toda instalación se hará en una pared de concreto y con caja de seguridad. La localización del equipo dependerá del área de cobertura a la cual se desea llevar el servicio. Si se desea llevar el servicio en áreas abiertas se colocará el AP en una oficina frente a una ventana para dispersar la señal hacia fuera de la oficina evitando la disipación y obstrucción de la señal inalámbrica.

## 6. Prueba de Conectividad

La fase de prueba toma en cuenta cuanta señal se está recibiendo, distancia de alcance, autenticación exitosa y tener acceso al AP. Para medir calidad de señal y alcance se utilizará algún dispositivo con capacidad inalámbrica. Se verificará que la conexión sea exitosa en la red con una cuenta autorizada. Se debe verificar que el AP *light weight* haya logrado una conexión exitosa con el controlador y se pondrá este en el grupo de wifi que le corresponda depende de los SSID (*Service Set Identifier*) que se vayan a transmitir en el área.

## 7. Autenticación

Las redes de empleados y estudiantes son uprrp-empleados y uprrp-estudiantes, respectivamente. Una vez conectado a esta red el cliente necesita autenticar con un portal donde utilizará su cuenta registrada en el *Active Directory*, ya sea su número de empleado o su número de estudiante. Si la persona desconoce su número de empleado se le orienta que debe llamar a la Oficina de Recursos Humanos para conocer el mismo y luego hacer una orden de servicio en la DTAA para hacer "reset" de la contraseña. Los estudiantes pueden buscar su información del PIN (*Pesonal identification number*) en la página de miupi.uprrp.edu. Las cuentas de estudiantes serán activadas al inicio de cada semestre y sólo los estudiantes activos tendrán acceso.

La red de visitantes, uprrp-visitor, tendrá cuentas temporeras para profesores y/o recursos visitantes. Se tiene que llenar una forma de creación de cuenta la que deberá estar firmada por el solicitante y un representante autorizado de la facultad que lo trae de visita. Esa hoja será entregada en la DTAA para su aprobación y creación.

## 8. Registro de MacAddress

El Registro de *MAC Address* es un proceso de seguridad utilizado para proveer acceso sólo a equipos que no proveen autenticación de cuenta. Se debe orientar al solicitante para que haga una orden de servicio utilizando *http://helpdesk.uprrp.edu* y proveer la lista en un archivo de texto utilizando el siguiente formato:

MAC,EXTENSION,EMAIL DE ENCARGADO ,MARCA,#PROPIEDAD,MAC@uprrp.edu,
MAC,MAC,DESCRIPCION,MAC, MAC,FACULTAD O OFICINA

Se creará una cuenta en el AD utilizando esta información, luego de creada la cuenta con la información provista se le entregará al solicitante una contraseña para la red uprrp-mac para que proceda a configurar el equipo.

### 9. Monitoreo Análisis de Rendimiento

El análisis de rendimiento se hará utilizando la plataforma de Cisco para manejar controladores y equipos *Cisco Prime NCS*. Para referencia del "IP Address" ver Anejo C-1. Este provee estadísticas de conexiones, usuarios y tráfico.

### 10. Parámetros Aceptables de Funcionamiento

Los AP tienen unas capacidades máximas para poder rendir su funcionamiento de la forma esperada. Es por esto que se han definido los siguientes parámetros:

- Usuarios conectados: 30 usuarios
- Tráfico: 70% del throughput total del Access Point

Cuando se alcanzan los límites establecidos, se entiende y se justifica por el uso, la adquisición y/o instalación de un AP nuevo. El listado de parámetros definido abajo es una guía y no una regla, cada caso será evaluado por los técnicos del sistema.

Al pasar los parámetros, se harán pruebas para determinar si se debe a un mal funcionamiento del equipo o si es necesario añadir otro AP para distribuir la carga.

### 11. Seguridad

Las redes que se proveen no tienen seguridad de cifrado y aunque las redes están configuradas para sólo hacer visible el proxy para los clientes, se debe ejercer precaución y/o cautela a la hora de transmitir información sensitiva utilizando este medio.

## H. Redes Cableadas

La red cableada tiene como propósito establecer la comunicación entre los edificios institucionales y la DTAA. Esta red permite a los usuarios acceder a los programados, servicios tecnológicos e información disponible electrónicamente y que son necesarios para cumplir con la misión de la UPR.

### 1. Evaluar Necesidad

Cuando las dependencias universitarias necesiten la instalación o reubicación de cableado estructurado, deberán enviar un comunicado a la DTAA, y el mismo se referirá a la Sección de Infraestructura y Redes. Estos proporcionarán los requisitos e informarán de las normas que deben cumplir para dicha instalación o reubicación.

Es importante que se determine el alcance del proyecto, es decir, si la instalación es una remodelación, adición a red existente o una red nueva. En el caso de ser remodelación, se trabajará en conjunto con la Oficina de Planificación y Desarrollo Físico (OPDF) para determinar la necesidad del usuario en términos de infraestructura. En caso de ser una adición a la red existente, se evaluará el área para determinar los recursos necesarios y la viabilidad del trabajo. Una red nueva de cableado se trabajará en conjunto con la OPDF y la firma de arquitectos, cuya función es el diseño de la infraestructura de comunicación. Luego de la evaluación se determinará si el trabajo será realizado por la oficina o por un suplidor.

### 2. Planificación

La planificación consta de diseño, recursos necesarios, así como un itinerario de las fases de ejecución. Durante este proceso se revisan y discuten los planos y el diseño proyectado. Se realizan reuniones periódicas con el personal involucrado en el proyecto para discutir el progreso del diseño y planificación del proyecto.

### 3. Ejecución

De haberse determinado que el personal de nuestra Oficina es el que hará la instalación se procede a realizar la misma. Si es un contratista el que va a realizar la instalación se procede al proceso administrativo de subasta y cuando se adjudique el contratista comenzará la instalación una vez se discuta con el personal de esta oficina. Se harán inspecciones visuales para revisar que el proyecto sigua el plan acordado.

### 4. Certificación

Los procesos de certificación se rigen por parámetros y mejores prácticas recomendadas y mencionadas en el *Building Industry Consulting Services International (BICSI)* y el cual también consta de pruebas que garanticen el buen funcionamiento del cableado. Todo proyecto realizado por esta oficina o por un contratista también debe tener sus debidas certificaciones. Estas certificaciones garantizan que ese cable ha pasado por los requisitos mínimos de funcionalidad. El proyecto se declarará terminado cuando culmine el proceso de revisar las certificaciones.

## I. Equipos de Telecomunicaciones

La interconexión física de todos los edificios del Recinto se logra a través de equipos de telecomunicaciones que son los que se encargan de redirigir todas las comunicaciones, sean estas internas o al Internet.

## 1. Configuración

La configuración básica de los equipos de telecomunicaciones se logra a través de un puerto de consola. Esta configuración incluye un usuario genérico, un servidor de RADIUS, configuración de SNMP, *IP address, default gateway*, DNS y configuración de SSH. Luego de la configuración básica se revisa la versión del equipo y se instala la más reciente y estable. Para garantizar acceso al equipo se le configura una cuenta local con el nombre de *netadmin*. Esta es una cuenta de emergencia, pues todo personal técnico debe tener una cuenta registrada en el servidor de RADIUS para autenticar a los equipos de telecomunicaciones. Para información adicional acerca de configuración de equipo favor ver manual del manufacturero. Los ejemplos de parámetros básicos de configuración se ilustran en el anejo C – Item 2.

## 2. Seguridad

Como medida de seguridad se configurará una lista de acceso que contiene los IP's autorizados para cambios. Sólo las computadoras en la lista (hosts) tendrán acceso a través de telnet (puerto: 23), https (puerto: 443) y ssh (puerto: 7785). En la medida que sea posible se debe utilizar el ssh (puerto 7785) sobre Telnet. Para el listado de direcciones de IP ver el anejo C-Item 3.

## 3. Instalación

El equipo de comunicaciones será instalado únicamente por personal de infraestructura de la DTAA. Deberán ir no menos de 2 personas para facilitar la instalación del mismo. Se deberá conectar este equipo en un cuarto de comunicación autorizado, preferiblemente, donde sólo personal de infraestructura y redes tenga acceso. Todo equipo debe ser conectado a un UPS para evitar fallos por fluctuaciones de voltaje. En caso de no haber UPS en el cuarto, la DTAA proveerá el mismo.

En caso de que un contratista, consultor o compañía externa realice trabajos de instalación o modificación, este deberá cumplir con las especificaciones mencionadas en la *sección VI-D de* "*Regulaciones y Estándares*", de este documento.

## 4. Prueba

La fase de prueba toma en cuenta la autenticación exitosa y tener acceso al equipo. Se realizará esta prueba de conectividad utilizando SSH (puerto 7785) o telnet desde las máquinas autorizadas. La autenticación se hace con una cuenta registrada en el servidor de RADIUS.

## 5. Mantenimiento

El mantenimiento del equipo, según contrato, se hará de la siguiente manera: se verificará periódicamente los *softwares releases* de todos los equipos de comunicaciones y se evaluarán, seleccionarán e instalarán únicamente aquellos que se identifiquen como estables y que no representen un riesgo de inestabilidad para el servicio. Las actualizaciones (*upgrades*) se instalarán el mismo día o mínimo cada dos meses, dependiendo de la urgencia y del riesgo de seguridad.

El reemplazo de algún componente electrónico defectuoso se hará según establecido por el contrato de mantenimiento o mediante una orden de compra aprobada por el Director Ejecutivo o su representante autorizado.

El cambio del *software releases* será llevado a cabo según se establece en la *sección VI-K- de "Periodo de Actualización"* de este documento.

### 6. Monitoreo (Análisis de Rendimiento)

El último paso en el proceso de instalación de equipos, es el de añadir el mismo a los programas de monitoreo disponibles. Este se llevará a cabo utilizando un SNMP (*Simple Network Management Protocol*) para estadísticas y/o ICMP *(Internet Control Message Protocol)* para verificar la conectividad, dependiendo de la herramienta utilizada.

### 7. Parámetros Aceptables de Funcionamiento

Los Equipos de Comunicaciones tienen unas capacidades máximas para poder rendir su funcionamiento de la forma esperada. Es por esto que hemos precisado un listado de parámetros, que al cumplirse se entiende y se justifica por el uso, la adquisición y/o instalación de un Equipo de Telecomunicación nuevo. El listado de parámetros definido abajo es una guía y no una regla, cada caso será evaluado por los técnicos del sistema.

- Tráfico: 70% por puerto
- CPU: 80%
- Paquetes por segundo: 30 mil paquetes por puerto
- Errores por puerto: 0%

Al pasar estos parámetros se harán pruebas para determinar si se debe a un mal funcionamiento del equipo o si es necesario reemplazar el mismo por uno de mayor capacidad.

## J. Servidores Físicos

Los servidores instalados en las facilidades de la DTAA le ofrecen a la comunidad universitaria acceso a los servicios necesarios para cumplir con la misión universitaria. Estos servicios son por ejemplo: aplicaciones administrativas, académicas, web, email, etc.

## 1. Instalación

La Sección de Infraestructura y Redes de la DTAA ha desarrollado un documento de configuración básica de servidores en el cual se especifican las configuraciones y opciones que cada servidor a ser instalado debe tener. Este documento se llama "***Normas y Procedimientos para la Configuración Básica de Servidores y Control de Acceso a través del Firewall*".** Todo servidor deberá ser instalado en un espacio apropiado, el cual debe contar con instalación eléctrica adecuada, control de temperatura, iluminación y puerta independiente, donde sólo esta Oficina tendrá acceso. En todos los servidores deben ser conectados al menos dos fuentes de poder, cada fuente debe ser conectada a un circuito eléctrico diferente para tener redundancia eléctrica. El servidor deberá estar en un equipo de *rack* e instalado en su lugar correspondiente con sus "*rapid rails" (*equipo para colocar servidores en gabinetes), todos los cables deberán correr por el brazo del riel y todos serán unidos con *velcro*. La conexión de mouse, teclado y pantalla se proveerá con un equipo KVM (*Keyboard, Video & Mouse)* instalado en el *rack*.

## 2. Servicio y Asignación de IP Address

El propósito de instalar un servidor en la red es el de proveer algún tipo de servicio. Al momento de instalar el servidor se debe tener un plan o estrategia de implementación del servicio que se quiere brindar. Todo servicio de red nuevo que se quiera implantar y no esté contemplado en la hoja de registro de servidores deberá ser consultado con ésta oficina para hacer un análisis de impacto y alcance del equipo. Toda persona que desee instalar un servidor en el *Server Farm* que necesite ser accesible a través del internet le será provisto un IP del segmento 180 o 223. El solicitante debe completar el formulario de inclusión al firewall para proveer la lista de los puertos TCP que utilizará su aplicación.

Algunos de los IPs reservados para estos usos son los ilustrados en el anejo C-4.

Si el servidor esta fuera de la DTAA se le asignará un IP dentro del rango perteneciente al edificio donde está localizado el mismo.

## 3. Monitoreo

El último paso para el proceso de instalación de servidores es añadir los mismos a los programas de monitoreo basado en lo mencionado en la *sección VI-G-8 de "Monitoreo Análisis de Rendimiento".*

### 4. Parámetros Aceptables de Funcionamiento

- CPU: 70% utilización
- Memoria: 75% uso
- Disco: 75% lleno
- Utilización de puertos

Al pasar estos parámetros se harán pruebas para determinar si se debe a un mal funcionamiento del equipo o si es necesario añadir procesadores, memoria o disco duro.

### 5. Mantenimiento

El sistema operativo de los servidores será actualizado utilizando los mecanismos provistos por el manufacturero. Los mismos serán evaluados e instalados el mismo día o como mínimo cada dos meses, dependiendo del carácter de prioridad y de acuerdo a la severidad que atienda la actualización. Las actualizaciones "firmware" de los componentes electrónicos del servidor, se analizarán y se evaluarán según las recomendaciones del manufacturero y se realizarán de ser necesarias.

El reemplazo de algún componente electrónico defectuoso se hará según establecido por el contrato de mantenimiento o mediante una orden de compra. Esta última requiere de la aprobación del Director de la DTAA o su representante.

Estas actualizaciones se harán cumpliendo con lo establecido en la *sección VI-K de "Periodo de Actualización",* de este procedimiento.

## K. Periodo de Actualización

En esta sección se establece una metodología para mantener en condiciones operativas todos los equipos de cómputo y telecomunicaciones y atender problemas técnicos que afecten o puedan afectar nuestras operaciones y las de los usuarios. La metodología será la siguiente:

| ACTIVIDAD | RESPONSABLE | REGISTRO |
|---|---|---|
| **1. Elaboración de Plan de Mantenimiento:** Elaborar un plan de mantenimiento para los equipos. El Plan debe contestar las siguientes preguntas:<br>• ¿Cuáles equipos se trabajarán?<br>• ¿Está el equipo en garantía o bajo contrato?<br>• ¿Qué trabajo se realizará a cada equipo? | Director de Servicios Técnicos en Tecnología de Información | Plan de Mantenimiento Preventivo Equipos de Cómputos y Comunicaciones (Anejo A) |

| | | |
|---|---|---|
| • ¿Cuánto tiempo aproximado será la suspensión del servicio?<br>• ¿Quién se afectará con el mantenimiento?<br>• ¿Cuál es la urgencia del mantenimiento y prioridad?<br>• ¿Cuál técnico realizará la tarea? | | |
| **2. Notificación del Mantenimiento Preventivo:** Someterá para aprobación el Plan de Mantenimiento con aproximadamente siete (7) días calendario antes del día seleccionado para dicho trabajo. Esta aprobación tendrá la firma del Director Asociado en Infraestructura Tecnológica o su representante. Si existe algún cambio se regresará a la actividad uno. | Director de Servicios Técnicos en Tecnología de Información | Plan de Mantenimiento Preventivo Equipos de Cómputos y Comunicaciones (Anejo A) |
| **3. Publicación del Calendario de Mantenimiento:** Si en el paso uno (1) se determina que los trabajos a realizar afectan a la comunidad universitaria se notificará a la comunidad o usuarios afectados previamente mediante un comunicado o notificación electrónica a los representantes técnicos de cada Facultad o usuarios. | Director de Servicios Técnicos en Tecnología de Información y Secretaria | WEB, EMAIL O CARTA |
| **4. Proceso de Mantenimiento Preventivo:** Cada equipo especificado en el Plan de Mantenimiento deberá ser desactivado de la herramienta de monitoreo oficial del Recinto. El Técnico asignado inicia el Mantenimiento Preventivo el cual puede ser superficial o completo según la programación y plan, si por algún motivo el equipo tiene que ser trasladado a otra área, se deberá notificar en el Plan de Mantenimiento. Luego se llenará una forma indicando el mantenimiento otorgado y hallazgos del mismo. | Técnico | Hoja de "Reporte de Incidentes y/o Mantenimiento" (Anejo B) |
| **5. Verificación del trabajo realizado:** Todo trabajo de mantenimiento deberá ser verificado garantizando la integridad del servicio. En caso de ser un mantenimiento realizado por terceros, entiéndase manufacturero o suplidor, el técnico de infraestructura en la DTAA deberá asegurarse de que se presente un informe por cada uno de los equipos a los que se le haga el mantenimiento de acuerdo a lo establecido contractualmente.<br>De ser un trabajo realizado por el técnico deberá reportarse al Director cualquier anomalía presentada para tomar las acciones respectivas. Una vez terminado el trabajo se activará el nodo en el programa de monitoreo. | Técnico o Responsable del Equipo o Director de Servicios Técnicos en Tecnología de Información | -- |

# VI. PREGUNTAS FRECUENTES

1. ***¿A quién aplica este procedimiento?***

Este procedimiento aplica al personal del área de infraestructura de la DTAA que esté autorizado para ejercer dichas funciones de mantenimiento y/o seguridad de la red.

2. ***¿Qué se requiere para que un usuario tenga acceso a la red inalámbrica del recinto?***

Para que un usuario tenga acceso a la red inalámbrica este debe tener una cuenta de empleado ó estudiante. En caso que sea un equipo que no soporte autenticación (ej. Televisores) el acceso se otorgará basándose en el *MAC Address*.

# VII. NORMATIVA LEGAL Y/O INSTITUCIONAL APLICABLE

- *Política Institucional Sobre el Uso Aceptable de los Recursos de Tecnología de la Información*, Certificación Núm. 35 (2007-2008) de la Junta de Síndicos.

- *Estándares para la Utilización Aceptable de Recursos de Tecnología Informática*, emitido el 4 de abril de 2008, por la Vicepresidencia de Investigación y Tecnología de la Universidad de Puerto Rico.

- *Normas y Procedimientos para la Configuración Básica de Servidores y Control de Acceso a través del Firewall*" del Recinto de Río Piedras, DTAA.

# VIII. OTRAS POLÍTICAS O PROCEDIMIENTOS INSTITUCIONALES RELACIONADOS

- Política Núm. TIG-008 sobre el *Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la Oficina de Gerencia y Presupuesto.

- Política Núm. TIG-003 sobre la *Seguridad de los Sistemas de Información* de la Oficina de Gerencia y Presupuesto.

# IX. APÉNDICES, FORMULARIOS Y ENLACES

Anejo A – Plan de Mantenimiento Preventivo Equipos de Cómputos y Comunicaciones
Anejo B – Reporte de Incidentes y/o Mantenimiento
Anejo C – IP Address

Anejo A – Plan de Mantenimiento Preventivo Equipos de Cómputos y Comunicaciones

Anejo A

| | DIVISION DE TECNOLOGIAS ACADEMICAS Y ADMINISTRATIVAS<br>PLAN DE MANTENIMIENTO PREVENTIVO EQUIPOS<br>DE COMPUTO Y COMUNICACIONES | Código: PM-FORM-01<br>Versión: 1.1<br>Fecha Aprobación: 2-mar-10<br>Página: 1 de 1 |
|---|---|---|

| No. | Código | Tipo de Equipo | Trabajo a Realizar | Fecha Programada | Efecto | | | Contacto |
|---|---|---|---|---|---|---|---|---|
| | | | | | Tiempo | Urgencia | Usuarios | |
| 1 | ejemplo | Servidor de http o web | Upgrade de memoria | 23-mar-2010 | 1 hr | low | All | rtorregrosa@uprrp.edu |
| 2 | ejemplo | Router building edge | Downgrade IOS | 23-mar-2010 | 2 hr | med | AMO Building | rgarcia@uprrp.edu |
| 3 | ejemplo | Servidor de Backup | Upgrade de kernel | 16-abr-2010 | 4 hr | high | All servers | roberto.rivera@uprrp.edu |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Revisado por: _____

Fecha: _____

Aprobado por: _____

Fecha: _____

Rev. lbb/10-mar-10\feb2013

Anejo B – Reporte de Incidentes y/o Mantenimiento

Anejo B

**Universidad de Puerto Rico**
**Recinto de Río Piedras**
**División de Tecnologías Académicas y Administrativas**

**Reporte de Incidente y/o Mantenimiento**

Número de Incidente: _____ Fecha(dd-mm-yyyy):_____
Nombre de Equipo: _____ Hora: _____

Tema (Incidente o Mantenimiento):_____
Tiempo de Duración: _____
Descripción de Equipo: _____
Quiénes se Afectaron: _____

Breve descripción del problema:

| |
|---|
| |

Acción tomada:

| |
|---|
| |

Sugerencia para evitar que se repita la situación (**si aplica**):

| |
|---|
| |

Atendido por:

_____
Nombre

Fecha (si es dif a la anterior): _____

Hora: _____

_____
Firma

rg/2009/2013

Anejo C – IP Address

## CERTIFICACION

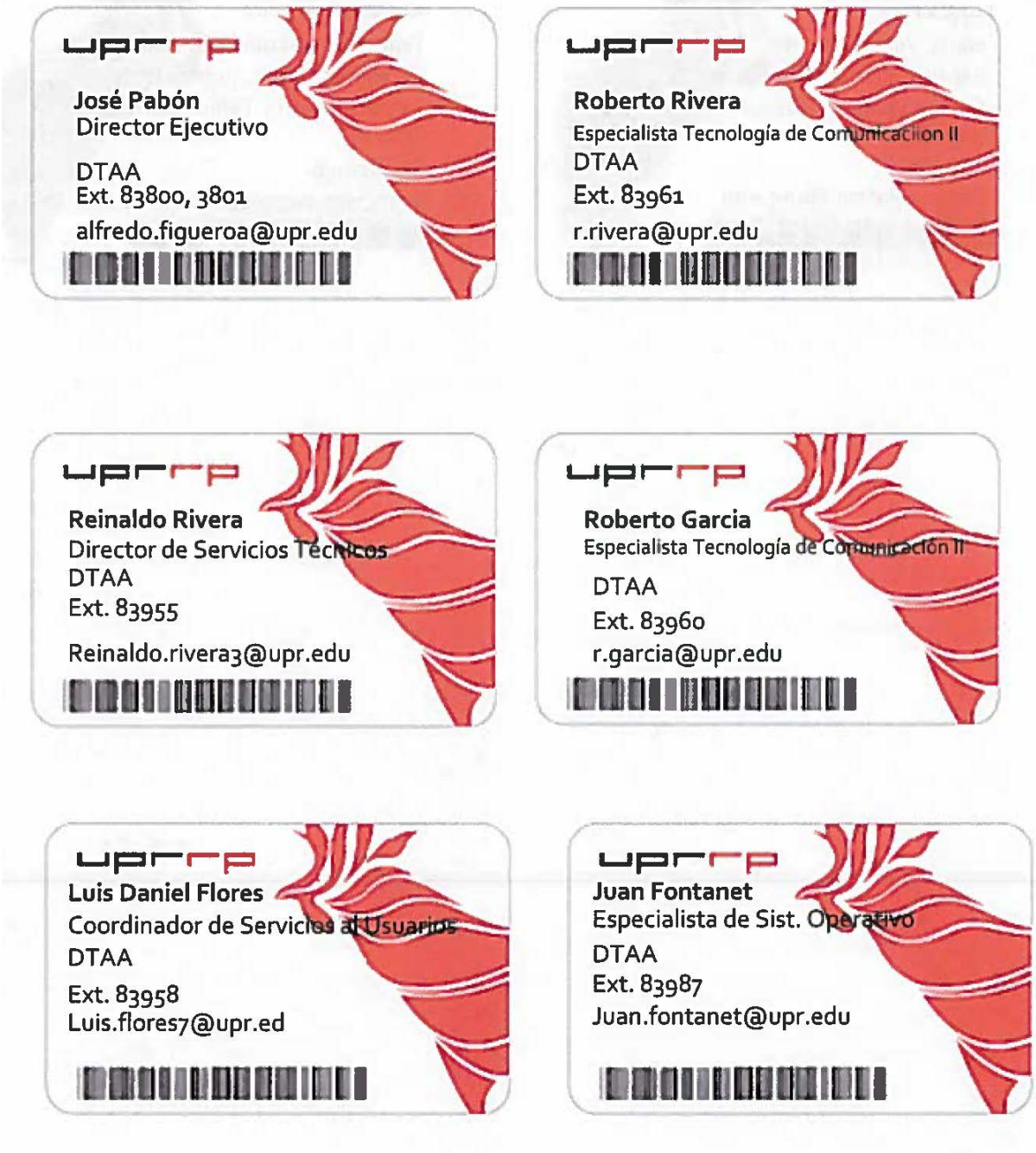
El "Anejo C" no se incluye en este procedimiento por razones de seguridad. Este anejo contiene una lista de "IP Address" y detalles de configuración de los servidores y dicha información es únicamente para el conocimiento y uso del personal de la Sección de Infraestructura como parte de sus funciones.

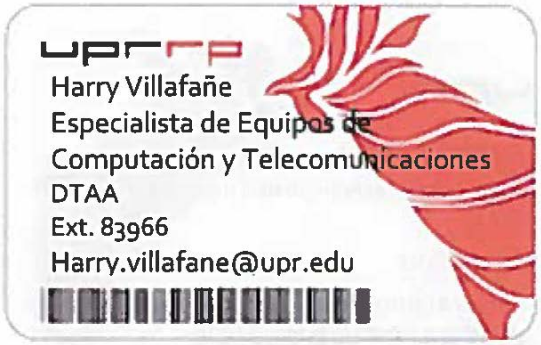
Este documento es un procedimiento interno de la DTAA y hacer pública dicha información podría poner en riesgo la seguridad de la red del Recinto. Se reservan la siguiente página como parte del anejo C.

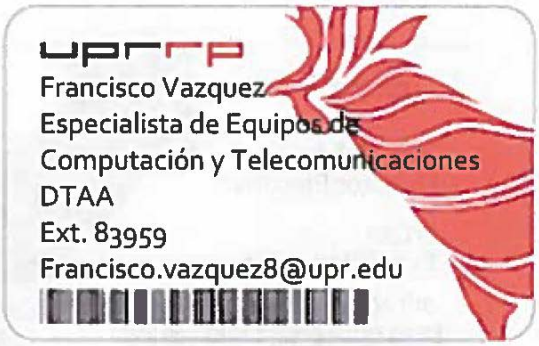
Firma:

Sr. José Pabón
Director Ejecutivo, DTAA
10/marzo/2017

# X. CONTACTOS


José Pabón
Director Ejecutivo
DTAA
Ext. 83800, 3801
alfredo.figueroa@upr.edu
Roberto Rivera
Especialista Tecnología de Comunicación II
DTAA
Ext. 83961
r.rivera@upr.edu
Reinaldo Rivera
Director de Servicios Técnicos
DTAA
Ext. 83955
Reinaldo.rivera3@upr.edu
Roberto Garcia
Especialista Tecnología de Comunicación II
DTAA
Ext. 83960
r.garcia@upr.edu
Luis Daniel Flores
Coordinador de Servicios al Usuarios
DTAA
Ext. 83958
Luis.flores7@upr.ed
Juan Fontanet
Especialista de Sist. Operativo
DTAA
Ext. 83987
Juan.fontanet@upr.edu


uprrp
Harry Villafañe
Especialista de Equipos de
Computación y Telecomunicaciones
DTAA
Ext. 83966
Harry.villafane@upr.edu


uprrp
Francisco Vazquez
Especialista de Equipos de
Computación y Telecomunicaciones
DTAA
Ext. 83959
Francisco.vazquez8@upr.edu