Normas y Procedimiento para la Creación de Cuentas de Sistemas de Información

Número:	RRP 4 2015 – 2016
Fecha:	29.02.2016
Firma:	
Autoridad Nominadora:	Carlos E. Severino Valdez, Ph.D.
Funcionario Responsable:	Director
Oficina Responsable:	División de Tecnologías Académicas y Administrativas

Tabla de Contenido

I. Introducción 3
II. Propósito 4
III. Interpretación y Definiciones 4
IV. Alcance 6
V. Responsabilidades 6
VI. Procedimiento 7
A. Criterios para la Creación de Cuentas 7
1.Cuenta de Administrador 7
2.Cuenta de Servicio 7
3.Cuenta Temporera 8
4.Cuentas del Fabricante 8
5.Cuentas de Usuarios 8
B. Acceso a los Sistemas 8
C. Parámetros de Creación de Cuentas: 9
1.Disposiciones generales 9
2.Disposiciones para cuentas temporeras y servicio 10
3.Disposiciones para cuentas del fabricante y/o aplicaciones 10
D.Seguridad 11
1.Seguimiento de actividad de las cuentas 11
VII. Preguntas Frecuentes 12
VIII. Normativa Legal y/o Institucional Aplicable 12
IX. Otras Políticas o Procedimientos Institucionales Relacionados 12
X. Historial 13
XI. Apéndices, Formularios y Enlaces 13
XII. Contactos 14

I. INTRODUCCIÓN

La División de Tecnologías Académicas y Administrativas (DTAA), adscrita a la Rectoría, tiene la responsabilidad de proteger y velar que la confidencialidad, integridad y disponibilidad de los recursos tecnológicos no se vea afectada por ataques a la red y a los sistemas de información del Recinto de Río Piedras de la Universidad de Puerto Rico (en adelante, el "Recinto"). Además, es responsable de la administración y monitoreo de la red y de establecer procedimientos que contribuyan a la seguridad de la misma.

Con el fin de proveer y mantener la seguridad de los sistemas de información en la Universidad de Puerto Rico, Recinto de Río Piedras, se establecen en este documento las normas y procedimiento que regirán la creación, administración y mantenimiento de las cuentas de los sistemas computadorizados.

También, se definen las responsabilidades del Director Ejecutivo de la DTAA y el Administrador del Sistema que incluye personal técnico de las diferentes unidades del Recinto, entiéndase administradores, técnicos y/o coordinadores de los recursos tecnológicos asignados a unidades fuera de la DTAA.

Unidad(es) Responsable(s)
División de Tecnologías Académicas y Administrativas

Otras Unidad(es) Concernida(s)
Oficinas del Recinto con personal técnico a su cargo

Puedo conseguir copia en:
DTAA

Fecha de Efectividad:
29/febrero/2016

Última Revisión
1/junio/2015

II. PROPÓSITO

El propósito de estas normas y procedimiento, es establecer y mantener un proceso uniforme para la creación, administración y mantenimiento de las cuentas de usuarios y administradores de sistemas computadorizados de información.

Además, establecer los controles de acceso, necesarios y adecuados para garantizar la confidencialidad, integridad y la disponibilidad de la información que se maneja en estos sistemas, con el fin primordial de evitar el acceso de forma no autorizada y/o maliciosa.

III. INTERPRETACIÓN Y DEFINICIONES

Para efectos de este documento, todo término utilizado para referirse a una persona o puesto se refiere a ambos géneros; el tiempo presente también incluye futuro; los términos en singular incluyen el plural. Las palabras y frases empleadas en este documento serán interpretadas según el contexto en que sean utilizadas y según han sido definidas para efectos de la misma. En el caso de aquellas palabras o frases no definidas, éstas tendrán el significado sancionado por el uso común y corriente.

Accesos	Se refiere, en este documento, a los privilegios concedidos a un usuario para la utilización de uno o más sistemas de información.
Administrador del Sistema	Personal técnico de la DTAA que tiene a su cargo uno o más sistemas de información. También, puede caer en esta categoría el personal técnico de las diferentes unidades del Recinto que tienen a su cargo la administración de servidores u otros equipos computarizados de la información correspondiente a su unidad de trabajo, entiéndase Decanato, Facultad, Escuela, Departamento u Oficina.
Contraseña	Información confidencial e individualizada, constituida por una cadena de caracteres, que junto al *Nombre de Usuario*, permiten el acceso a uno o más sistemas de información.
Cuenta de Administrador	Se refiere a toda cuenta con privilegios de acceder y modificar uno o más sistemas operativos, utilidades y pantallas de configuración de los sistemas de información.
Cuenta de Fabricante	Se refiere a toda cuenta configurada de fábrica en un sistema. Usualmente, estas cuentas tienen privilegio de administrador y no pueden ser borradas.
Cuenta Interna	Se refiere a toda cuenta que sea necesaria para el buen funcionamiento de un *sistema*. Usualmente estas cuentas tienen, únicamente, los privilegios mínimos necesarios para cumplir su función y no son

usadas por los administradores, fabricantes, personal de servicio o usuarios.

Cuenta de Servicio	Se refiere a toda cuenta que utiliza el fabricante o proveedor de servicio para acceder al sistema en aquellas ocasiones en que así sea requerida para ofrecer apoyo técnico a los administradores de Tecnologías de información. Usualmente, estas cuentas tienen privilegio de administrador y se mantienen inactivas.
Cuenta de Usuario	Se refiere a toda cuenta con privilegios de acceder un sistema no descrito en el inciso anterior y que a esos efectos, los administradores han determinado que se proveerá el acceso a los que así lo necesiten.
Nombre de Usuario ("Username")	Se refiere a la cuenta única que se asigna a un usuario para que junto a la *contraseña* y los debidos privilegios, obtenga acceso a uno o más *sistemas de información.*
Personal Técnico	Personal del Recinto que tiene a su cargo deberes y responsabilidades correspondientes para brindar asistencia a equipos y/o programados de su unidad. Éstos también, pudieran tener servidores a su cargo.
Seguridad	El término seguridad, en este documento, se refiere al área de la informática y seguridad de la información que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta, como: bases de datos, normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable en donde se puedan identificar y eliminar vulnerabilidades.
Sistema(s) de Información	Incluye, pero no se limita, a: (1) servidores y computadoras personales, (2) programados, aplicaciones, utilidades y pantallas de configuración, (3) Equipos de comunicaciones ("Switches", "Routers", "Access Points", etc.), (4) Unidades de teléfonos y sistemas telefónicos analógicos o digitales ("PBX's"), Sistemas "Voice Over IP" o "Voice Over Wireless LAN", etc.
Usuario	Entiéndase decanato, facultad, escuela, oficina o departamento o persona autorizada a acceder datos o recursos en un *sistema de información*, pero que no tiene privilegios de administrador.

IV. ALCANCE

Este procedimiento aplica al personal de la División de Tecnologías Académicas y Administrativas (DTAA) el cual tiene a su cargo la administración y monitoreo de los recursos de la red, así como una serie de equipos donde se mantienen las bases de datos de los sistemas administrativos y académicos del Recinto.

También aplica al personal técnico destacado en las diferentes unidades del Recinto, entiéndase Decanato, Facultad, Escuela, Departamento u Oficina, que tienen a su cargo la administración de servidores y/o aplicaciones que requieren de la otorgación de cuentas. Este personal deberá velar por la seguridad, confidencialidad y disponibilidad de los equipos y servicios que administran como parte de los recursos para las operaciones académicas y/o administrativas del Recinto.

V. RESPONSABILIDADES

Director Ejecutivo de la DTAA	1. Evaluar y autorizar las solicitudes de cuentas con privilegios de administrador. Los accesos otorgados a estas cuentas son restringidos y autorizados, según las funciones y responsabilidades del solicitante que requiera cuenta con privilegios de administrador para acceder y modificar uno o más sistemas operativos, utilidades y pantallas de configuración de los sistemas de información, así como creación de usuarios, asignación de contraseñas, etc.
Administrador del Sistema	1. Otorgar los accesos a los sistemas una vez aprobada la "*Solicitud de Cuentas de los Sistemas de Información del Recinto de Rio Piedras*". Este deber lo ejecuta el Administrador del Sistema de la DTAA, pero los Administradores de las demás unidades del Recinto debieran aplicar medidas similares como método de control de acceso a sus sistemas. 2. Revisar semanalmente, o según sea necesario, los registros de auditoría de los servidores, sistemas operativos, aplicaciones y servicios. 3. Informar a sus superiores y tomar acción inmediata cuando surjan eventos identificados como críticos en la red y que reflejen acciones sin autorización o actividades ilegales. Eventos que no requieren acción inmediata, deben ser calendarizados para ser verificados en un periodo de una semana.

4. Someter informes y mantener registros detallados de los resultados de sus revisiones, las cuales debe realizar semanalmente o según sea necesario.

5. Asignar nombre de usuario ("username") y contraseña y comunicar los mismos por vías seguras que no contengan indicaciones externas de su contenido.

   Ejemplo: Nunca deberá comunicarse por teléfono o facsímil y si se utiliza el correo electrónico, la línea de "asunto" no debe indicar que el mensaje contiene un nombre de usuario o contraseña.

6. Mantener la seguridad de la cuenta que le sea asignada únicamente a su persona.

7. Hacer buen uso de la misma de acuerdo con los propósitos para la cual le fue autorizada, según sus funciones y responsabilidades como administrador, de tal forma que pueda mantener la seguridad, confiabilidad y funcionalidad de los sistemas y equipos que administra en su unidad de trabajo.

VI. PROCEDIMIENTO

A. Criterios para la creación de cuentas

Para establecer y mantener un procedimiento uniforme para la creación, administración y mantenimiento de las cuentas asignadas a los usuarios y administradores de sistemas computadorizados en el Recinto, es necesario evaluar el otorgamiento de las mismas bajo los siguientes criterios y/o clasificaciones:

1. **Cuenta de Administrador** - Se otorgará una cuenta con privilegio de administrador a todo empleado del Recinto que, por la naturaleza de sus funciones, requiere este nivel de acceso para realizar las mismas.

2. **Cuenta de Servicio** - Se otorgará una cuenta de servicio a todo fabricante, distribuidor, consultor, contratista o proveedor de servicio que así lo requiera para ofrecer servicios de consultoría o apoyo técnico a los administradores de Tecnologías de Información del Recinto.

3. **Cuenta Temporera** - Se creará una cuenta interna cuando el administrador del sistema lo estime necesario para el funcionamiento apropiado del sistema. Éstas tendrán un tiempo de expiración determinado por la oficina solicitante.

4. **Cuentas del Fabricante** – Cuentas incluidas en los equipos, programas y sistemas. Quedan excluidas (de los criterios de creación) por ser requeridas para el buen funcionamiento del sistema; sólo podrá editarse la contraseña.

5. **Cuentas de Usuarios** – El administrador creará una cuenta de usuario a todo estudiante, empleado docente o no docente, a tiempo completo o parcial, a consultores, etc., que tenga una necesidad debidamente justificada y autorizada de acceder a un sistema de información.

B. Acceso a los Sistemas

1. Toda persona que requiera de una cuenta, deberá completar el formulario "*Solicitud de Cuentas de los Sistemas de Información del Recinto de Río Piedras*". El mismo está disponible a través de la página Web de la UPR-Recinto de Río Piedras o en la DTAA

2. Cada usuario tendrá una cuenta que se relacionará directa y únicamente con su persona.

3. Los accesos otorgados estarán basados en la naturaleza de la función y responsabilidades del solicitante, como: configuración del sistema, creación de usuarios, asignación de contraseñas, etc.

4. El usuario que requiera privilegios de alta jerarquía dentro de los niveles de seguridad de un sistema (Ejemplo: "Administrator" o "Root"), se les proveerán los mismos a su cuenta particular, la cual no compartirán con ningún otro usuario.

5. Los privilegios para los usuarios externos deberán ser solicitados a través del supervisor o representante de la compañía que ofrecerá el servicio. Éste deberá completar el formulario "*Solicitud de Cuentas de los Sistemas de Información del Recinto de Río Piedras*", el cual debe ser aprobado por el Director Ejecutivo de la DTAA. El Administrador del Sistema a cargo de la seguridad, otorgará los accesos aprobados y será responsable de suspender la cuenta una vez el servicio requerido sea completado.

6. Todo formulario de solicitud de cuenta será archivado con la documentación del usuario.

C. Parámetros de creación de cuentas:

1. Disposiciones generales

a. Las contraseñas con roles de usuario regular estarán compuestas por un mínimo de 8 caracteres, los cuales incluirá una letra mayúscula y números.

b. Las contraseñas para usuarios con roles de administrador estarán compuestas por un mínimo de 15 caracteres, en los sistemas que así lo permitan. o el máximo de caracteres permitidos por el sistema operativo, los cuales deben incluir una letra mayúscula, caracteres especiales y números.

c. Se le hará llegar a cada usuario una contraseña temporera inicial generada al azar. Estas contraseñas se asignarán de forma compleja de deducir por otros, utilizando: dígitos, letras mayúsculas y minúsculas, caracteres especiales, etc., si el sistema así lo permite.

d. El usuario tendrá que cambiar su contraseña inmediatamente al acceder al sistema por primera vez.

e. Para toda cuenta de los sistemas administrativos y Administradores de Sistemas la contraseña expirará cada noventa (90) días, a partir de la fecha inicial en que el usuario establece la misma, por lo que tendrá que crear una nueva contraseña al término de este tiempo.

f. El número máximo de intentos fallidos para introducir la contraseña correctamente se limitará a seis (6) veces, en cuyo caso, la cuenta del usuario quedará bloqueada hasta que suceda una de las siguientes:

   1) Un administrador desbloquee la cuenta.

   2) Se espere el tiempo establecido de 30 minutos para que la misma se desbloquee automáticamente

g. Se debe establecer, en los sistemas que así lo permitan, un historial de contraseñas de al menos cuatro (4) más recientes para evitar su repetición.

h. Cada usuario será responsable de mantener la confidencialidad de la contraseña de su cuenta y de cualquier acción o acceso indebido que se haga desde la misma.

i. El nombre de usuario ("username") y contraseña inicial se comunicarán por vías seguras y no deberá tener indicaciones externas de su contenido. Por ejemplo: Nunca deberá comunicarse por teléfono o facsímil y, si se utiliza el correo electrónico, la línea de "asunto" no debe indicar que el mensaje contiene un nombre de usuario o contraseña.

j. Para los sistemas OpenVMS se recomienda crear un registro alterno de usuarios (SYSUAFALT.DAT), con nombre de usuario y contraseña para evitar el acceso no autorizado desde la consola. La cuenta y contraseña se guardará en un sobre sellado en un lugar seguro para utilizarse en caso de emergencia. De requerir usar la cuenta, la persona encargada de mantener el sobre sellado, procederá a registrar la utilización de la misma. Una vez termine, el administrador del sistema procederá a cambiar la contraseña de la cuenta, guardarla en un sobre sellado y devolverla al lugar designado.

2. Disposiciones para cuentas temporeras y servicio

a. Las cuentas temporeras y de servicio serán regidas por las disposiciones generales, excepto el tiempo de expiración de la cuenta. Las cuentas temporeras tendrán un tiempo de expiración determinado por la oficina solicitante. Las cuentas de servicio tendrán un término de caducidad basado en el término del contrato establecido.

3. Disposiciones para cuentas del fabricante y/o aplicaciones

a. Las contraseñas del fabricante incluidas en los equipos, programas y sistemas, especialmente, aquellas de administradores o usuarios con accesos amplios, se sustituirán al momento de hacer la instalación o configuración de los mismos.

b. Las contraseñas del fabricante o cuentas para aplicaciones requerirán un mínimo de veinte (20) caracteres, las cuales se asignarán de forma compleja de deducir por otros, utilizando: dígitos, letras mayúsculas y minúsculas, caracteres especiales, etc. Las mismas no tendrán periodo de expiración.

c. Las cuentas del fabricante y sus nuevas contraseñas se guardarán en un sobre sellado para ser enviado a bóveda externa y se utilizará solamente en caso de emergencia. Al momento de requerirse el sobre, el Administrador del Sistema de la DTAA, una vez termine de utilizar la contraseña, deberá cambiar la misma y guardarla en sobre sellado y enviarlo nuevamente a bóveda externa. Las únicas personas autorizadas para solicitar el sobre son: el Director Ejecutivo y el Director del Área de Infraestructura, ambos de la DTAA. El personal técnico del Recinto, localizado fuera de la DTAA y con funciones de administrador, deberá adoptar medidas similares.

D. Seguridad

1. Seguimiento de Actividad de las Cuentas

a. Al interrumpirse el uso de un sistema durante 10 minutos, automáticamente dejará de mostrar la información en la pantalla, requiriendo la re-autenticación del usuario para obtener acceso nuevamente al mismo, salvo para aquellos sistemas en que esto no sea posible o porque por sus características, se fije otro límite, ya sea inferior o superior.

b. Cada Administrador de Sistema será responsable de verificar y evaluar, anualmente, las cuentas creadas por ellos y eliminar aquellas inactivas, según aplique.

c. Para los sistemas que así lo permitan, se mantendrán registros de auditoría de las transacciones realizadas por los usuarios para manejar el control, verificación e investigación. Estos registros contendrán, al menos, la siguiente información:

   1) Fecha y hora del evento;
   2) Sistema;
   3) Dirección IP de la fuente y del destino (si aplica);
   4) Nombre del usuario;
   5) Tipo de evento;
   6) Si el intento de acceso fue autorizado o denegado;
   7) Resultado, efecto o consecuencia del evento.

d. El Administrador del Sistema a cargo de la seguridad revisará los Registros de Auditoría de los servidores, sistemas operativos, aplicaciones y servicios que incluyen, pero no se limitan a:

   1. Sistemas Operativos: OpenVMS, Linux, Mac OS o Windows
   2. Servidores: Domain Controller, DNS/WINS/DHCP, FireWall, Web Server, Mail Server
   3. Aplicaciones: HRS, SIS, Compras, BlackBoard
   4. SYSLOG devices, SYSLOG Severity Codes, etc.

e. Cada Administrador de Sistema a cargo de la seguridad de un sistema y/o servidor, realizará revisiones de los mismos semanalmente o según sea necesario e informará a sus superiores y tomará acción inmediata para eventos identificados como críticos en la ejecución y función de la red y eventos que reflejen acciones sin autorización o actividades ilegales.

Eventos que no requieran acción inmediata, deben ser calendarizados para ser verificados en un periodo de una semana. El Administrador del Sistema mantendrá registros detallados de los resultados de sus revisiones y rendirá informes a su supervisor inmediato, de ser necesario.

VII. PREGUNTAS FRECUENTES

a. ¿Dónde puedo conseguir el formulario de solicitud de cuentas?

El formulario con nombre de "*Solicitud de Cuentas de los Sistemas de Información del Recinto de Río Piedras*" puede conseguirse a través de la página Web de la UPR- Recinto de Río Piedras o en la DTAA.

b. ¿A quién aplica este procedimiento?

Este procedimiento aplica a todo personal técnico que tenga a su cargo funciones de asignación de cuentas a los usuarios ya sea para los sistemas de su unidad o sistemas a nivel del Recinto.

VIII. 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.

IX. 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.

X. HISTORIAL

N/A

XI. APÉNDICES

- **APÉNDICE 1** - Solicitud de Cuenta para los Sistemas de Información del Recinto de Río Piedras

Apéndice 1:

División de Tecnologías Académicas y Administrativas

Solicitud de Cuenta para los Sistemas de Información del Recinto de Río Piedras

☐ Nueva ☐ Modificar ☐ Cancelar

☐ Estudiante ☐ Docente ☐ No Docente

A. **Cuenta que solicita** (sólo puede marcar una opción, en el caso de solicitar otros sistemas debe llenar un formulario por cada sistema)

☐ SIS* ☐ Dominio RRP
☐ HRS* ☐ Administrador Servidores
☐ LICENCIAS* ☐ Share Point
☐ PROPIEDAD* ☐ Otros _____
*Requiere un segundo formulario

☐ Email UPR EDU (GAE)
☐ organizacional _____
☐ personal _____
☐ Email UPRRP EDU (equipos de oficina)

B. Datos del Solicitante (Favor de escribir en letra de molde)

_____
Nombre Inicial Apellido Paterno Apellido Materno

_____
Título de Puesto

_____
Facultad o Decanato

_____
Oficina o Departamento

_____
Teléfono o extensión

_____
Correo electrónico (oficial, sino alterno)

C. Certificación

Certifico que la información aquí brindada es correcta y que el uso de la cuenta estará limitado al propósito y las funciones indicadas en esta solicitud. Tengo conocimiento y acepto la Política Sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico Recinto de Río Piedras, promulgada mediante la Certificación Núm. 035-2007-2008, firmada el 19 de febrero de 2008. Entiendo que el incumplimiento de cualquiera de las disposiciones que se establecen en dicha política estará sujeto a las sanciones académicas, administrativas y legales aplicables. Entiendo que si no utilizo la cuenta por un periodo de seis meses la misma será cancelada automáticamente. De necesitarla requerirá llevar acabo nuevamente el proceso de solicitud.

_____
Firma del Solicitante Fecha

D. SOLO PARA EMPLEADOS

D 1 _____
NOMBRE EN LETRA DE MOLDE del Director del Departamento u Oficina o Decano del Solicitante (No puede ser la misma del solicitante)

D 2 _____
FIRMA del Director del Departamento u Oficina o Decano del Solicitante (No puede ser la misma del solicitante) Fecha

D 3 _____
Firma del Gerente del Sistema Administrativo Fecha
(EN CASO DE QUE EL SOLICITANTE SEA EL MISMO COORDINADOR, ENTONCES LA AUTORIDAD NOMINADORA DEBE FIRMAR)

E. Para Uso Oficial de la DTAA

☐ Nueva ☐ Modificada

☐ Añadir Cuenta ☐ Cancelada

Cuenta Asignada: _____

Contraseña: _____

Número de Operador: _____

Número de ID: _____

Fecha de Expiración (si aplica): _____

Trabajada por (en letra de molde): _____

Firma: _____

Registrada por: _____

Notificada por: _____

Fecha: _____

Rev 18/feb/2015

X. CONTACTOS

Alfredo Figueroa
Director Ejecutivo
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext. 83801, 83800
alfredo.figueroa@upr.edu

Roberto García
Especialista en Tecnología de Comunicación
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext. 83950, 83800
r.garcia@upr.edu

Reinaldo Rivera
Director Sección de Infraestructura
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext. 83950, 83800
reinaldo.rivera3@upr.edu

Juan Fontanet
Especialista en Sistema Operativo
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext. 83987
juan.fontanet@upr.edu

Luis D. Flores
Coordinador de Servicios al Usuario
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext. 83950, 83800
luis.flores7@upr.edu

Wanda Rivera
Coordinadora de Servicios al Usuario
División de Tecnologías Académicas
y Administrativas (DTAA)
787-764-0000 Ext 83973
wan.rivera@upr.edu