



*Secretaría*

**MANUEL A. TORRES NIEVES**

SECRETARIO DEL SENADO

A handwritten signature in black ink, appearing to read "Manuel A. Torres Nieves", is written over the printed name and title.

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- Expediente
- Dar Cuenta
- Registrar y Procesar

*Senado*  
DE PUERTO RICO

EL CAPITOLIO  
PO Box 9023431  
San Juan, Puerto Rico  
00902-3431

T: 787.722.3460  
787.722.4012  
F: 787.723.5413  
E: mantorres@senadopr.us  
W: www.senadopr.us

## REFERIDO A:

### COMISIONES PERMANENTES

---

- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico y Planificación
- Urbanismo e Infraestructura
- Jurídico Penal
- Jurídico Civil
- Agricultura
- Recursos Naturales y Ambientales
- Comercio y Cooperativismo
- Turismo y Cultura
- Trabajo, Asuntos del Veterano y Recursos Humanos
- Bienestar Social
- Asuntos Municipales
- Recreación y Deportes
- Banca, Asuntos del Consumidor y Corporaciones Públicas
- Desarrollo de la Región del Oeste
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario
- Asuntos Federales
- De la Montaña
- Ética

### COMISIONES ESPECIALES

---

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

### COMISIONES CONJUNTAS

---

- Informes Especiales del Contralor
- Donativos Legislativos de Puerto Rico
- Internado Córdova-Fernós
- Internado Pilar Barbosa
- Internado Ramos Comas
- Código Penal
- Revisión y Reforma del Código Civil
- Alianzas Público Privadas
- Auditoría Fiscal y Manejo Fondos Públicos
- Revisión Continua Código Penal y Reforma de las Leyes



*[Handwritten initials]*

Iniciales

*Oficina del Presidente*

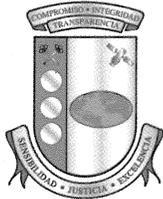
Katherine Erazo  
CHIEF OF STAFF

Fecha 6 de octubre de 2011

Referido a Manuel Torres

- Para su información
- Evaluar y recomendar
- Para trabajar y contestar directamente
- Dar cuenta al cuerpo
- Para otorgar contrato
- Para nombramiento
- Autorizado

14800



Estado Libre Asociado de Puerto Rico  
**Oficina del Contralor**

RECIBIDO  
OFIC. PRESIDENTE SENADO  
THOMAS RIVERA SCHATZ

2011 OCT -6 AM 10:54

Yesmín M. Valdivieso

Contralora

6 de octubre de 2011

**A LA MANO**

**PRIVILEGIADA Y CONFIDENCIAL**

Hon. Thomas Rivera Schatz  
Presidente  
Senado de Puerto Rico  
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-12-04* del Centro de Tecnología de Información del Recinto Universitario de Mayagüez de la Universidad de Puerto Rico aprobado por esta Oficina el 29 de septiembre de 2011. Publicaremos dicho *Informe* en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,

  
Yesmín M. Valdivieso

Anejo

RECIBIDO SECRETARIA  
SENADO DE P.R.  
2011 OCT -7 AM 8:55

DA 15102



**INFORME DE AUDITORÍA TI-12-04**

29 de septiembre de 2011

**Universidad de Puerto Rico**

**Recinto Universitario de Mayagüez**

**Centro de Tecnología de Información**

(Unidad 5520 - Auditoría 13230)

Período auditado: 14 de octubre de 2008 al 20 de marzo de 2009

AD-15PR



## CONTENIDO

	Página
<b>INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....</b>	<b>3</b>
<b>RESPONSABILIDAD DE LA GERENCIA .....</b>	<b>5</b>
<b>ALCANCE Y METODOLOGÍA .....</b>	<b>6</b>
<b>OPINIÓN.....</b>	<b>6</b>
<b>RECOMENDACIONES .....</b>	<b>7</b>
A LA JUNTA DE SÍNDICOS DE LA UNIVERSIDAD DE PUERTO RICO .....	7
AL PRESIDENTE DE LA UNIVERSIDAD DE PUERTO RICO.....	7
AL RECTOR DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ .....	7
<b>CARTAS A LA GERENCIA.....</b>	<b>14</b>
<b>COMENTARIOS DE LA GERENCIA.....</b>	<b>14</b>
<b>AGRADECIMIENTO.....</b>	<b>15</b>
<b>RELACIÓN DETALLADA DE HALLAZGOS.....</b>	<b>16</b>
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	16
HALLAZGOS EN EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ DE LA UNIVERSIDAD DE PUERTO RICO .....	17
1 - Deficiencias en el control y en el mantenimiento de las cuentas para acceder los sistemas administrativos del RUM, falta de activación de los registros para examinar los eventos de seguridad, y documentación inadecuada sobre las revisiones de los eventos de intentos fallidos.....	17
2 - Deficiencias en el uso del formulario para solicitar acceso a los sistemas administrativos del RUM, y en los controles para solicitar acceso a los sistemas de información de los departamentos de Matemáticas y de Ingeniería Eléctrica y Computadoras.....	21

3 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de los departamentos de Matemáticas e IEC .....	26
4 - Contraseñas almacenadas sin estar cifradas .....	29
5 - Falta de almacenamiento de los respaldos en un lugar seguro fuera de los predios donde estaba ubicado el centro de computadoras del Departamento de IEC .....	30
6 - Falta de normas y de procedimientos escritos, y procedimientos sin aprobar .....	31
7 - Deficiencias en los cuartos de distribución del cableado ( <i>wiring closets</i> ), y falta de actualización del diagrama esquemático de la red del RUM.....	35
8 - Limitaciones en la aplicabilidad de la <i>Guía RUMNET</i> , y falta de documentación de los análisis realizados a las actividades inusuales en los registros de la red, y de un itinerario para el mantenimiento de los equipos conectados a esta.....	40
9 - Falta de un registro de los servidores autorizados a ser instalados en la red del RUM, y de problemas ocurridos en los sistema operativos.....	43
<b>ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS QUE ACTUARON DURANTE EL PERÍODO AUDITADO.....</b>	<b>45</b>
<b>ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO.....</b>	<b>46</b>

Estado Libre Asociado de Puerto Rico  
**OFICINA DEL CONTRALOR**  
San Juan, Puerto Rico

29 de septiembre de 2011

Al Gobernador, al Presidente del Senado  
y a la Presidenta de la Cámara de Representantes

Realizamos una auditoría de las operaciones del Centro de Tecnología de Información (CTI) del Recinto Universitario de Mayagüez (RUM) de la Universidad de Puerto Rico (UPR) para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Efectuamos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

Determinamos emitir dos informes de esta auditoría. Este último informe contiene el resultado del examen de los controles de acceso y de los controles para la red de comunicaciones (red). El primer informe se emitió el 11 de mayo de 2010 y contiene el resultado del examen de los controles internos establecidos para la administración del programa de seguridad, el desarrollo y el control de cambios a las aplicaciones, la continuidad de servicio, y la documentación del *Sistema de Información Estudiantil (SIE)* (*Informe de Auditoría TI-10-16*).

**INFORMACIÓN SOBRE LA UNIDAD AUDITADA**

El 20 de enero de 1966, se aprobó la *Ley Núm. 1, Ley de la Universidad de Puerto Rico*, según enmendada, para reorganizar la estructura funcional de la UPR. Mediante la *Ley Núm. 16*

del 16 de junio de 1993, se enmendó el Artículo 3 de la *Ley Núm. 1* para eliminar el Consejo de Educación Superior como cuerpo rector de la UPR y crear la Junta de Síndicos. Esta gobierna y administra el sistema universitario de Puerto Rico.

Mediante la *Ley Núm. 1*, se concedió autonomía académica y administrativa al RUM y se integraron a este todas las escuelas, los colegios, las facultades, los departamentos, los institutos, los centros de investigación y demás dependencias que funcionaban bajo el Colegio de Agricultura y Artes Mecánicas de la UPR. También quedaron integrados al RUM la Estación Experimental Agrícola y el Servicio de Extensión Agrícola, en lo administrativo y en lo programático. Estas dos unidades son examinadas por separado y nuestra Oficina rinde informes individuales para cada una de ellas. El RUM es administrado por un Rector nombrado por la Junta de Síndicos.

Los recursos para sus gastos de funcionamiento provienen de asignaciones legislativas, fondos federales, donativos e ingresos propios. Para el año fiscal 2008-09 el presupuesto del RUM ascendió a \$203,024,810 y el presupuesto operacional del CTI ascendió a \$1,811,655.

El RUM se compone de 9 unidades institucionales: Rectoría, 7 decanatos (3 administrativos y 4 académicos) y 1 Centro de Investigaciones. El RUM tiene 3 áreas principales: la administrativa, la investigativa y la académica. La persona responsable de los sistemas de información computadorizados en el área administrativa es el Ayudante del Rector para Asuntos en Tecnología y Director del CTI. Además, el RUM cuenta con 32 coordinadores responsables de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicaciones en los departamentos. Estos coordinadores le responden directamente a sus decanos o directores de departamentos.

El CTI tiene 32 empleados y está compuesto por 5 unidades principales: Servicios al Usuario, Servicios Técnicos, Unidad de Análisis y Programación, Operaciones, y Grupo de Desarrollo Web. También cuenta con un Administrador de Base de Datos, un Oficial de Control, un Gerente de Sistemas y un Especialista en Sistemas Operativos. El RUM tiene una computadora principal para procesar la información de los sistemas *Financial Resources System (FRS)*, *Human Resources System (HRS)* y *SIE*.

El **ANEJO 1** contiene una relación de los miembros principales de la Junta de Síndicos que actuaron durante el período auditado. El **ANEJO 2** contiene una relación de los funcionarios principales que actuaron durante dicho período.

El RUM cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.uprm.edu>. Esta página provee información acerca de la entidad y de los servicios que presta.

### **RESPONSABILIDAD DE LA GERENCIA**

La gerencia de todo organismo gubernamental debe considerar los siguientes *Diez Principios para Lograr una Administración Pública de Excelencia*. Estos se rigen por principios de calidad y por los valores institucionales:

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.
2. Mantener una oficina de auditoría interna competente.
3. Cumplir con los requisitos impuestos por las agencias reguladoras.
4. Adoptar un plan estratégico para las operaciones.
5. Mantener el control presupuestario.
6. Mantenerse al día con los avances tecnológicos.
7. Mantener sistemas adecuados de archivo y de control de documentos.
8. Cumplir con el *Plan de Acción Correctiva* de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.
9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.
10. Cumplir con la *Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, lo cual incluye divulgar sus disposiciones a todo el personal.

El 27 de junio de 2008, mediante la *Carta Circular OC-08-32*, divulgamos la revisión de los mencionados diez principios, establecidos en nuestra *Carta Circular OC-98-09* del 14 de abril de 1998. Se puede acceder a ambas cartas circulares a través de nuestra página en Internet: <http://www.ocpr.gov.pr>.

### ALCANCE Y METODOLOGÍA

La auditoría cubrió del 14 de octubre de 2008 al 20 de marzo de 2009. En algunos aspectos examinamos operaciones de fechas posteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias.

Para efectuar la auditoría utilizamos la siguiente metodología:

- entrevistas a funcionarios, a empleados y a particulares
- inspecciones físicas
- examen y análisis de informes y de documentos generados por la unidad auditada
- examen y análisis de informes y de documentos suministrados por fuentes externas
- pruebas y análisis de procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

### OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del CTI en lo que concierne a la evaluación de los controles de acceso y de los controles para la red del RUM no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 9**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

## RECOMENDACIONES

### A LA JUNTA DE SÍNDICOS DE LA UNIVERSIDAD DE PUERTO RICO

1. Ver que el Presidente de la Universidad de Puerto Rico cumpla con la **Recomendación 2** de este *Informe*. **[Hallazgos del 1 al 9]**

### AL PRESIDENTE DE LA UNIVERSIDAD DE PUERTO RICO

2. Ver que el Rector del RUM cumpla con las **recomendaciones de la 3 a la 7** de este *Informe*. **[Hallazgos del 1 al 9]**

### AL RECTOR DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ

3. Ejercer una supervisión eficaz sobre el Ayudante del Rector para Asuntos en Tecnología y Director del CTI para que este se asegure de que:

- a. El Especialista en Sistemas Operativos II:

- 1) Identifique periódicamente las cuentas de acceso que no han sido utilizadas por un período mayor de 30 días, y notifique a los directores y a los supervisores que autorizaron dichas cuentas, que se procederá a inactivar las mismas. **[Hallazgo 1-a.1)a) y b)]**
- 2) Se asegure de que todas las cuentas de acceso creadas en la computadora principal se identifiquen con el nombre de los usuarios a quienes están asignadas. **[Hallazgo 1-a.1)c) y d)]**
- 3) Restrinja el tiempo de acceso correspondiente a las cuentas de acceso de los usuarios de la computadora principal, según las funciones y las responsabilidades de estos y a las necesidades de servicio del RUM. **[Hallazgo 1-a.2)]**
- 4) Se asegure de que todas las cuentas de acceso creadas en la computadora principal, con privilegios de administrador, contengan un mínimo de 15 caracteres. **[Hallazgo 1-a.3)]**

- 5) Revise todos los registros que provee el sistema operativo de la computadora principal, relacionados con los eventos de seguridad sobre el uso de las cuentas de acceso de los usuarios, y documente por escrito o por un medio electrónico externo los procesos realizados y los resultados obtenidos. Dicha información deberá retenerse conforme a la reglamentación aplicable. **[Hallazgo 1-b.]**
  - 6) Se asegure de requerir el *Formulario de Solicitud* debidamente completado en todas sus partes y aprobado por los funcionarios concernientes antes de crear las cuentas de acceso en el sistema. Además, de mantener los mismos bajo su custodia, organizados y accesibles. **[Hallazgo 2-a.]**
- b. El Coordinador de Servicios al Usuario II del CTI:
- 1) Redacte y remita para aprobación las normas y los procedimientos necesarios para reglamentar los procesos sobre la administración, la seguridad y el uso de los sistemas de información computadorizados que se detallan en el **Hallazgo 6-a.3).**
  - 2) Mantenga evidencia de los análisis realizados mediante las herramientas de monitoreo a la red, de los registros de actividades inusuales y de las fallas potenciales de seguridad. **[Hallazgo 8-b.]**
  - 3) Se asegure de mantener una bitácora para identificar y documentar los problemas ocurridos del sistema operativo de los servidores y cómo los mismos fueron resueltos. **[Hallazgo 9-b.]**
- c. La Especialista en Sistemas Operativos II del CTI revise y remita para aprobación los procedimientos *Eliminación de Cuentas para ex funcionarios, Seguridad en FRS y Seguridad en HRS*. **[Hallazgo 6-b.2)]**

- d. El Director de Servicios Técnicos II:
- 1) Actualice el diagrama esquemático de la red del RUM, para que se incluyan en el mismo los servidores, el *firewall*<sup>1</sup>, los *routers*<sup>2</sup>, los *switches*<sup>3</sup>, el *backbone*<sup>4</sup>, los equipos inalámbricos y las computadoras principales, y la manera en que estos equipos se interconectan. **[Hallazgo 7-b.]**
  - 2) Establezca un itinerario formal para efectuar el servicio de mantenimiento preventivo a cada equipo conectado a la red. **[Hallazgo 8-c.]**
  - 3) Se asegure de mantener un registro de los servidores autorizados a ser instalados en la red del RUM y que el mismo incluya la información requerida por la Sección 2.5 de la *Guía Operacional Red de Comunicaciones de Datos RUMNET v.2.1.* diciembre de 2006 (*Guía RUMNET*). **[Hallazgo 9-a.]**
- e. Revise y remita para aprobación la *Guía RUMNET* para que la misma sea de aplicabilidad para las unidades institucionales del RUM. **[Hallazgo 8-a.]**
4. Ver que el Decano de la Facultad de Artes y Ciencias se asegure de que el Director del Departamento de Matemáticas ejerza una supervisión efectiva sobre el Coordinador de Servicios al Usuario I para que:
- a. Prepare y remita para aprobación un formulario para el control de las solicitudes de cuentas de acceso a los recursos computadorizados del Departamento de

---

<sup>1</sup> Sistema que se coloca entre una red de comunicaciones e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad y autenticación, entre otros.

<sup>2</sup> Dispositivo que distribuye el tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y tablas de direccionamiento.

<sup>3</sup> Dispositivo de comunicación central que conecta dos o más segmentos de red y permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

<sup>4</sup> Línea de transmisión más grande que transporta la información recopilada de líneas más pequeñas que están interconectadas con ella.

Matemáticas, para el personal administrativo y docente de dicho Departamento. Dicho formulario deberá proveer un espacio para la aceptación y la aprobación del Director del Departamento de Matemáticas. **[Hallazgo 2-b.1)a) y b)]**

- b. Configure los parámetros de seguridad en los servidores para que se:
  - 1) Requiera al usuario un cambio de contraseña cuando acceda por primera vez a la red del Departamento de Matemáticas. **[Hallazgo 2-b.1)c)]**
  - 2) Requiera, al menos, un mínimo de 10 días para que el sistema le permita al usuario cambiar su contraseña nuevamente. **[Hallazgo 3-a.1)]**
  - 3) Restrinja a los usuarios el poder repetir las últimas cinco contraseñas utilizadas. **[Hallazgo 3-a.1)]**
  - 4) Desactiven automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la red. **[Hallazgo 3-a.1)]**
  - 5) Requiera que las contraseñas estén compuestas de 8 caracteres de combinaciones de letras, números, caracteres especiales y alfanuméricos. **[Hallazgo 3-a.1)]**
- c. Establezca un plan para el mantenimiento y el control de las cuentas de acceso de manera que se asegure el cambio de contraseñas periódicamente por parte de los usuarios, se desactiven las cuentas que no se hayan utilizado por un período determinado y se eliminen las que no se hayan utilizado. **[Hallazgo 3-a.3)a) y c)]**
- d. Redacte y remita para aprobación las normas y los procedimientos escritos para que al momento de renuncia, separación o traslado de un usuario se le notifique oportunamente a la persona encargada de la seguridad de los sistemas para que proceda a eliminar o desactivar la cuenta de acceso correspondiente. **[Hallazgos 3-a.3)b) y 6-a.1)]**

- e. Configurar los servidores y los programas para que se mantengan cifradas las contraseñas de las cuentas de acceso de los usuarios para evitar la lectura de las mismas. **[Hallazgo 4]**
  - f. Revise los procedimientos *Información sobre Seguridad, Plan de Contingencias de Sistemas de Información y Redes de Comunicación*, y remita los mismos al Director del Departamento de Matemáticas para aprobación. **[Hallazgo 6-b.1]**
  - g. Realice las gestiones necesarias para que se identifiquen los cables, de manera que se pueda determinar con facilidad a qué computadora pertenecen y corregir a tiempo los problemas de comunicación. **[Hallazgo 7-a.4)a]**
  - h. Prepare y remita para aprobación el diagrama esquemático de la infraestructura de la red del Departamento que incluya lo siguiente: el *firewall*, los *routers*, los *switches*, el *backbone*, los accesos remotos y las conexiones inalámbricas, entre otros. **[Hallazgo 7-a.4)b]**
  - i. Se asegure de tomar las medidas necesarias para que en todos los cuartos de distribución de cableado se mantengan las condiciones ambientales y los controles de acceso físico adecuados. **[Hallazgo 7-a.4)c) y d)]**
5. Ver que el Decano de la Facultad de Ingeniería se asegure de que:
- a. El Director del Departamento de Ingeniería Eléctrica y Computadoras (IEC) ejerza una supervisión efectiva sobre el Especialista en Telecomunicaciones I para que:
    - 1) Revise y remita para aprobación la *Solicitud de Cuentas* para que se incluya un espacio para la aceptación y la aprobación del Director del Departamento. **[Hallazgo 2-b.2)a]**
    - 2) Prepare los procedimientos escritos sobre la creación, la cancelación, el uso y el control de las cuentas con privilegio de acceso remoto a los usuarios y remita los mismos al Director del Departamento para aprobación. **[Hallazgo 2-b.2)b]**

- 3) Configure las siguientes opciones de seguridad requerida en los referidos servidores:
- a) Requiera un mínimo de 10 días para que el sistema le permita al usuario cambiar su contraseña. **[Hallazgo 3-a.1)]**
  - b) Restrinja que los usuarios puedan repetir las últimas cinco contraseñas utilizadas. **[Hallazgo 3-a.1)]**
  - c) Desactive automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la red. **[Hallazgo 3-a.1)]**
  - d) Requiera que las contraseñas estén compuestas de 8 caracteres de combinaciones de letras, números, caracteres especiales y alfanuméricos. **[Hallazgo 3-a.1)]**
  - e) Activar las opciones contenidas en la pantalla de políticas de auditorías (*Audit Policies*) en los servidores. **[Hallazgo 3-a.2)]**
  - f) Duplique periódicamente la información almacenada en los medios electrónicos que se utilizan como parte de las operaciones normales del IEC. Mantenga una copia de dicha información y de la documentación de los programas en un lugar seguro fuera de los predios del IEC. **[Hallazgo 5]**
  - g) Prepare y remita para aprobación las normas y los procedimientos escritos necesarios para que al momento de renuncia, separación o traslado de un usuario de sus funciones se efectúe una notificación oportuna a la persona encargada de la seguridad de los sistemas de información para proceder a eliminar o desactivar la cuenta de acceso de dicho usuario. **[Hallazgo 6-a.1)]**

- h) Se asegure de que no se utilicen los cuartos de distribución de cableado para almacenar equipo de las computadoras. **[Hallazgo 7-a.2)a]**
  - i) Prepare y remita para aprobación el diagrama esquemático de la infraestructura de la red del Departamento que incluya lo siguiente: el *firewall*, los *routers*, los *switches*, el *backbone*, los accesos remotos y las conexiones inalámbricas, entre otros. **[Hallazgo 7-a.2)b]**
  - j) Realice las gestiones necesarias para que se identifiquen los cables, de manera que se pueda determinar con facilidad a qué computadora pertenecen y corregir a tiempo los problemas de comunicación. **[Hallazgo 7-a.2)c]**
  - k) Se asegure de tener extintores de incendios accesibles en los cuartos de cableado. **[Hallazgo 7-a.2)d]**
- b. El Director de Ingeniería Civil ejerza una supervisión efectiva sobre el Coordinador de Servicios Técnicos al Usuario I para que:
- 1) Se asegure de tener extintores de incendios accesibles en los cuartos de cableado. **[Hallazgo 7-a.3)a]**
  - 2) Prepare y remita para aprobación el diagrama esquemático de la infraestructura de la red del Departamento que incluya lo siguiente: el *firewall*, los *routers*, los *switches*, el *backbone*, los accesos remotos y las conexiones inalámbricas, entre otros. **[Hallazgo 7-a.3)b]**
  - 3) Se asegure de tomar las medidas necesarias para que en todos los cuartos de distribución de cableado se mantengan debidamente identificados los cables utilizados para las conexiones entre los diferentes equipos de telecomunicaciones, y los controles de seguridad de acceso físico y ambientales adecuados. **[Hallazgo 7-a.3)c) y d)]**

6. Tomar las medidas necesarias para asegurarse de que el Decano de Administración ejerza una supervisión efectiva sobre el Director de la Oficina de Propiedad para que:
  - a. Ejercer una supervisión eficaz sobre el Registrador de Datos II, para cifrar las contraseñas de las claves de acceso de los usuarios del Sistema de Inventario de Propiedad para evitar la lectura de las mismas. **[Hallazgo 4]**
  - b. Prepare y remita para aprobación las normas y los procedimientos sobre las políticas para la seguridad del Sistema de Inventario de Propiedad que establezca los requerimientos para la asignación y la eliminación de cuentas de acceso a dicho sistema. **[Hallazgo 6-a.2]**
  - c. Establezca los controles físicos necesarios para mantener separada el área en donde se encuentran ubicados los equipos de telecomunicaciones principales del RUM del área de servicios auxiliares del Edificio de Telefónica. **[Hallazgo 7-a.1]**
7. Imparta instrucciones a los decanos y a los directores de departamento del RUM para que velen que sus correspondientes coordinadores de informática se aseguren de cumplir con la *Guía RUMNET* para mantener una uniformidad en los procesos relacionados con la instalación, la configuración y la documentación de la red del RUM. **[Hallazgo 8-a.]**

### CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este *Informe* se remitió al Dr. Miguel A. Muñoz Muñoz, entonces Rector del RUM, para comentarios, en carta del 29 de octubre de 2010. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Dr. Jorge Iván Vélez Arocho, ex-Rector del RUM, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por este.

### COMENTARIOS DE LA GERENCIA

El entonces Rector contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 30 de noviembre de 2010. Sus comentarios fueron considerados en la redacción final de

este *Informe*; y se incluyen en la sección de la segunda parte de este *Informe*, titulada HALLAZGOS EN EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ DE LA UNIVERSIDAD DE PUERTO RICO.

El ex-Rector no contestó el borrador de los **hallazgos** de este Informe que le fuera remitido para comentarios en carta del 29 de octubre de 2010 y en carta de seguimiento del 17 de noviembre de 2010.

#### AGRADECIMIENTO

A los funcionarios y a los empleados del RUM, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor  
Por: *Fernando M. Valderrama*

## RELACIÓN DETALLADA DE HALLAZGOS

### CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas. Estos se clasifican como principales o secundarios. Los principales incluyen desviaciones de disposiciones sobre las operaciones de la unidad auditada que tienen un efecto material, tanto en el aspecto cuantitativo como en el cualitativo. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves.

Los hallazgos del informe se presentan según los atributos establecidos conforme a las normas de redacción de informes de nuestra Oficina. El propósito es facilitar al lector una mejor comprensión de la información ofrecida. Cada uno de ellos consta de las siguientes partes:

**Situación** - Los hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.

**Criterio** - El marco de referencia para evaluar la situación. Es principalmente una ley, un reglamento, una carta circular, un memorando, un procedimiento, una norma de control interno, una norma de sana administración, un principio de contabilidad generalmente aceptado, una opinión de un experto o un juicio del auditor.

**Efecto** - Lo que significa, real o potencialmente, no cumplir con el criterio.

**Causa** - La razón fundamental por la cual ocurrió la situación.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los exfuncionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe; y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ DE LA UNIVERSIDAD DE PUERTO RICO, de forma objetiva y conforme a las normas de nuestra

Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, este prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

## HALLAZGOS EN EL CENTRO DE TECNOLOGÍA DE INFORMACIÓN DEL RECINTO UNIVERSITARIO DE MAYAGÜEZ DE LA UNIVERSIDAD DE PUERTO RICO

Los **hallazgos** de este *Informe* se clasifican como principales.

### **Hallazgo 1 - Deficiencias en el control y en el mantenimiento de las cuentas para acceder los sistemas administrativos del RUM, falta de activación de los registros para examinar los eventos de seguridad, y documentación inadecuada sobre las revisiones de los eventos de intentos fallidos**

- a. El RUM tenía una computadora principal para procesar la información de los sistemas *Financial Resources System (FRS)*, *Human Resources System (HRS)* y *Sistema de Información Estudiantil (SIE)*. En esta se mantenía una base de datos con 904 cuentas de acceso activas.
  - 1) El examen de las 904 cuentas reveló que:
    - a) Ciento setenta y cinco cuentas<sup>5</sup> permanecían activas a pesar de que las mismas no habían sido utilizadas por más de 3 meses. El tiempo transcurrido sin tener actividad fluctuó entre 91 y 3,641 días consecutivos.
    - b) Se habían creado 96 cuentas<sup>5</sup> que nunca se utilizaron.
    - c) Se habían creado 29 cuentas<sup>5</sup> con un nombre de usuario que no permitía identificar a la persona que hacía uso de la misma.
    - d) Once cuentas<sup>5</sup> no tenían el nombre de usuario.

---

<sup>5</sup> Las cuentas de acceso se incluyeron en el borrador de los **hallazgos** de este *Informe*, remitido al entonces Rector y al ex Rector para comentarios.

- 2) El examen de 45 de las 904 cuentas de acceso, relacionado con los parámetros establecidos en el sistema operativo de la computadora principal, reveló que a estas no se les había restringido el tiempo para acceder a los sistemas correspondientes, conforme a las responsabilidades y a los deberes que los usuarios tenían asignados, y a las necesidades de servicios de estos. Dichas cuentas estaban configuradas para permitir a los usuarios acceder los recursos de dichos sistemas, los 7 días de la semana y las 24 horas del día.

En la Sección II, Puntos Generales, de las *Normas de Seguridad Lógica de los Sistemas Administrativos*, aprobadas en julio de 2007 por el Director del CTI, se establece, entre otras cosas, que cualquier cuenta podrá ser desactivada, de no tener actividad por un período de 30 días o más. Además, se establece que cualquier cuenta que no vaya a ser usada por un largo período será desactivada para minimizar la posibilidad de accesos no autorizados a través de dichas cuentas.

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipo y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, se establece que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Dicha norma se instrumenta, en parte, mediante lo siguiente:

- El uso de las opciones para restringir el tiempo de acceso y controlar los accesos que proveen los distintos sistemas operativos
- La documentación adecuada de las cuentas de acceso creadas que permita identificar el nombre del usuario responsable de usar la misma

- La notificación inmediata al encargado de la seguridad de datos del cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para la cancelación de su cuenta de acceso.
- 3) El examen de las 27 cuentas de acceso correspondientes a los empleados del CTI que tenían acceso a dicha computadora, reveló que 3 cuentas de acceso que tenían privilegios de administrador estaban configuradas para permitir a los usuarios de las mismas, escribir menos de 15 caracteres al establecer sus contraseñas.

En la Sección III, Políticas de Contraseñas, de las *Normas de Seguridad Lógica de los Sistemas Administrativos*, se establece, entre otras cosas, que las contraseñas expiran cada 60 días y deben tener 8 caracteres de largo para usuarios y 15 para los usuarios con privilegios.

- b. La computadora principal tenía un sistema que permite identificar y revisar eventos de seguridad ocurridos, relacionados con el uso de las cuentas de acceso de los usuarios, tales como: eventos de accesos, autorización de las cuentas, ataques contra la seguridad del sistema, conexiones o desconexiones con cuentas con privilegios, creación de cuentas, salidas de sistemas protegidos, eliminación de cuentas protegidas, instalaciones, intentos fallidos (*login fails*), entradas exitosas al sistema, salidas del sistema, programa para controlar la red, uso de las cuentas con privilegios, modificación de parámetros del sistema y modificación del horario del sistema.

El examen sobre el uso de dicho sistema reveló que solo 2 de los 15 eventos de seguridad (intentos fallidos y uso de las cuentas con privilegios) eran auditados por la Especialista de Sistemas Operativos II.

En la Sección IX, Auditorías de las Cuentas, de las *Normas de Seguridad Lógica de los Sistemas Administrativos*, se establece, entre otras cosas, que periódicamente se llevará a cabo una auditoría de las cuentas de los usuarios, la cual tendrá como propósito detectar

irregularidades en el acceso y en el uso de las cuentas. Además, se establece que la auditoría se hará a base de las bitácoras y las alarmas del sistema, las cuales serán revisadas por la Especialista en Sistemas Operativos del Centro de Cómputos.

Las situaciones comentadas en el **apartado a.** propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **apartado b.** limita la detección temprana de vulnerabilidades, errores críticos o problemas con los servidores que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, limita a la gerencia de los registros necesarios para identificar accesos no autorizados y el uso indebido de los sistemas computadorizados para que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas en los **apartados a. y b.** se debían, en parte, a que el Director del CTI no veló que la Especialista en Sistemas Operativos II cumpliera con los controles de seguridad requeridos por las *Normas de Seguridad Lógica de los Sistemas Administrativos* para el mantenimiento de las cuentas de acceso. Tampoco veló que estuviesen activadas todas las opciones de seguridad para obtener y monitorear los eventos de seguridad ocurridos con el uso de las cuentas de acceso de los usuarios.

En la carta del entonces Rector, este nos indicó, entre otras cosas, lo siguiente:

[...] Anualmente se lleva a cabo un procedimiento de renovación de cuentas, en el cual los directores y supervisores someten a CTI que cuentas aún están autorizadas para que se mantengan activas. [sic]

**[Apartado a.1)a]**

El 7 de noviembre de 2010 se revisaron las cuentas que tienen todos los privilegios en el servidor [...] y todas tienen el indicador AUDIT habilitado.

[sic] **[Apartado b.]**

Consideramos las alegaciones del Rector con respecto al **apartado a.1)a)** del **Hallazgo**, pero determinamos que el mismo prevalece, porque no es una práctica recomendable para la seguridad de los sistemas, esperar un año para verificar cuáles cuentas están autorizadas. Además, en nuestro examen encontramos más de 60 cuentas que habían estado inactivas por más de un año.

**Hallazgo 2 - Deficiencias en el uso del formulario para solicitar acceso a los sistemas administrativos del RUM, y en los controles para solicitar acceso a los sistemas de información de los departamentos de Matemáticas y de Ingeniería Eléctrica y Computadoras**

- a. El RUM utiliza el *Formulario de Solicitud, Renovación o Cambio de Cuentas (Formulario de Solicitud)*, revisado en diciembre de 1997, para tramitar y controlar todas las solicitudes, las renovaciones y los cambios de cuentas de acceso a los sistemas administrativos *FRS*, *HRS* y *SIE*. Estos sistemas residían en una computadora principal y el control de acceso a los mismos lo mantenía la Especialista en Sistemas Operativos II.

El examen sobre la utilización del *Formulario de Solicitud* para 45 de las 904 cuentas de acceso con derechos a acceder los sistemas administrativos del RUM, reveló las siguientes deficiencias:

- 1) No se encontró, ni fue suministrada, evidencia de que se hubiera utilizado el *Formulario de Solicitud* para la creación de 5 de las 45 cuentas de acceso (11 por ciento).
- 2) Para la solicitud y la aprobación de las restantes 40 cuentas de acceso se utilizó el *Formulario de Solicitud*. El examen de estos formularios reveló que les faltaba parte de la información requerida, según se indica:

<b>INFORMACIÓN REQUERIDA</b>	<b>CANTIDAD DE FORMULARIOS</b>
Fecha de creación de la cuenta	17
Marca de cotejo de aprobación o no del acceso	9

INFORMACIÓN REQUERIDA	CANTIDAD DE FORMULARIOS
Firma del funcionario que solicitó el acceso	5
Firma del Director del CTI	2

- b. El RUM tenía 32 coordinadores responsables de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicación en los diferentes departamentos. Cada coordinador era responsable de proveer, mantener y controlar los derechos de acceso a los diferentes recursos computadorizados que mantenía el departamento para el cual trabajaba. Estos coordinadores le respondían directamente al decano o director del departamento correspondiente.

Examinamos los controles existentes en el proceso de otorgar acceso a los recursos computadorizados que mantienen el Departamento de Matemáticas y el de IEC.

1) En el Departamento de Matemáticas:

- a) No se había diseñado un formulario de control para la solicitud y la aprobación de las cuentas de acceso del personal administrativo y docente. Solo se mantenía la *Solicitud de cuentas estudiantes graduados Departamento de Matemáticas RUM* y la *Solicitud de cuentas estudiantes sub-graduados Departamento de Matemáticas RUM*, para el control de acceso.
- b) La *Solicitud de cuentas estudiantes graduados Departamento de Matemáticas RUM* no proveía un espacio para la aprobación de la cuenta por parte del Director del Departamento.
- c) En la *Solicitud de cuentas estudiantes graduados Departamento de Matemáticas RUM* se registraba la cuenta (*User name*) y la contraseña (*password*) del estudiante graduado. Sin embargo, el sistema no se había configurado para hacer obligatorio el cambio de la contraseña, una vez el usuario accede el mismo por primera vez con su cuenta. Esto, para que la contraseña del estudiante graduado sea confidencial.

- 2) El Departamento de IEC mantenía la *Solicitud de Cuentas* para el control de acceso a los recursos computadorizados de dicho Departamento. El examen reveló que:
- a) La *Solicitud de Cuentas* no proveía un espacio para la aprobación de la cuenta por parte del Director del Departamento.
  - b) En dicho Departamento existían 5 líneas de conexión por módems para tener acceso a un servidor de autenticación. Dichas líneas se establecieron para que tanto los estudiantes como el personal docente y el administrativo pudieran realizar trabajos desde sus casas. El examen de 44 cuentas de acceso asignadas a los usuarios que tenían privilegios de acceso remoto a dicho servidor reveló que:
    - (1) No se había documentado la solicitud, la justificación de estas cuentas ni la aprobación, por parte del Director del Departamento, para accederlas remotamente.
    - (2) No se habían eliminado del Sistema 17 cuentas de acceso<sup>6</sup> remoto que pertenecían a exempleados y a personal trasladado a otras áreas del RUM que no deberían tener acceso remoto a los recursos del Departamento. El tiempo transcurrido desde las separaciones y los traslados de los empleados fluctuó entre 13 y 121 meses.

En la Sección VI, Inciso 15, de la *Política Institucional y Procedimiento para el Uso Ético Legal de las Tecnologías de Información de la Universidad de Puerto Rico*, aprobada el 10 de febrero de 2000 por la Junta de Síndicos de la Universidad de Puerto Rico, se establece, entre otras cosas, que ninguna cuenta de nueva creación será autorizada sin el *Formulario de Solicitud de Renovación, Creación o Cambio de Cuenta*. Este deberá ser completado en su totalidad y en los espacios provistos deberán aparecer las firmas requeridas.

---

<sup>6</sup> Véase la nota al calce 5.

En la Sección IV, Solicitud de cuentas para el Sistema Administrativo, de las *Normas de Seguridad Lógica de los Sistemas Administrativos* se establece, que para obtener una cuenta en el sistema administrativo la persona deberá completar el *Formulario de Solicitud* en todas sus partes y llevarlo al centro de cómputos.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se disponen las directrices generales que permiten a las agencias establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejen. En dicha política se establece que la información y los programas de aplicación utilizados en las operaciones de las agencias deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización. Estas normas se instrumentan, en parte, mediante:

- El establecimiento de controles de acceso rigurosos a la red, a los programas y a los archivos, incluido el uso de formularios para solicitar la creación, la modificación o la eliminación de cuentas de acceso a los diferentes recursos disponibles a través de la red, para cada usuario.
- El mantenimiento de registros confiables y actualizados de las cuentas solicitadas y autorizadas.
- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.
- El establecimiento de normas y procedimientos específicos para la asignación del privilegio de acceso remoto a los usuarios, donde se incluya, entre otras cosas, la justificación por escrito para el otorgamiento de dicho privilegio.

Las situaciones que se comentan impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. También

propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, pueden propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades

Las situaciones comentadas en el **apartado a.** se debían, en parte, a que el Director del CTI no veló que la Especialista en Sistemas Operativos II mantuviera los documentos organizados, accesibles y completados en todas sus partes.

Las situaciones que se comentan en el **apartado b.1)a) y b)** se debían, en parte, a que el Director del Departamento de Matemáticas no le había requerido al Coordinador de Servicios al Usuario I<sup>7</sup> el diseñar, para su consideración y aprobación, un formulario para la solicitud y la aprobación de cuentas de acceso, que aplicara de manera uniforme tanto a los estudiantes como al personal docente y al administrativo, y que incluyera un espacio para la autorización de la cuenta solicitada por parte del Director del Departamento.

La situación comentada en el **apartado b.1)c)** se debía, en parte, a que el Coordinador de Servicios al Usuario I<sup>7</sup>, asignado al Departamento de Matemáticas, había dejado a la discreción de los estudiantes el cambio de contraseñas.

La situación comentada en el **apartado b.2)a)** se debía en parte a que el Director del Departamento de IEC no le había requerido al Especialista en Telecomunicaciones I<sup>8</sup> el rediseñar la *Solicitud de Cuentas* para que incluya un espacio para la aprobación por parte del Director del Departamento.

Las situaciones comentadas en el **apartado b.2)b)** se debían, en parte, a que el Director del Departamento de IEC no había promulgado normas ni procedimientos escritos sobre la creación, el uso y el control de las cuentas con privilegios de acceso remoto.

---

<sup>7</sup> Nombre del puesto que ocupaba el coordinador responsable de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicación en el Departamento de Matemáticas.

<sup>8</sup> Nombre del puesto que ocupaba el coordinador responsable de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicación en el Departamento de IEC.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones para velar por que los formularios de cuentas sean completados según requerido por los procedimientos establecidos.  
**[Apartado a.]**

Se impartirán instrucciones para establecer los requerimientos para documentar y establecer procedimientos escritos. **[Apartado b.]**

### **Hallazgo 3 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de los departamentos de Matemáticas e IEC**

a. El examen sobre los parámetros de seguridad y el control de acceso establecidos en un servidor<sup>9</sup> del Departamento de Matemáticas, y en tres servidores<sup>9</sup> del Departamento de IEC, reveló las siguientes deficiencias:

1) En las pantallas *Account Policy* de los cuatro servidores no se habían activado los parámetros para:

- Requerir un mínimo de 10 días para que el sistema le permita al usuario cambiar su contraseña nuevamente (*Minimum password age*).
- Evitar que un usuario vuelva a utilizar la misma contraseña en determinado tiempo (*Enforce password history*).
- Deshabilitar las cuentas de acceso por el número de intentos para acceder a los recursos de la red sin éxito (*No account lockout*).

Además, en dos servidores<sup>9</sup> del Departamento de IEC y en un servidor<sup>9</sup> del Departamento de Matemática no se habían activado los parámetros para definir el mínimo de caracteres requeridos en la contraseña de los usuarios (*Minimum password Length*).

---

<sup>9</sup> El nombre de los servidores se incluyó en el borrador de los **hallazgos** de este *Informe*, remitido al entonces Rector y al ex Rector para comentarios.

- 2) No se habían activado las opciones correspondientes a las políticas de auditoría (*Audit Policies*) a nivel local en los tres servidores<sup>10</sup> del Departamento de IEC, para que el sistema produzca un registro cuando ocurran los siguientes eventos:
- el encendido y apagado de la computadora (*Restart and Shutdown*)
  - el acceso a archivo y a objetos (*File/Object Access*)
  - los cambios a las políticas de seguridad (*Security Policy Changes*)
  - el acceso al directorio de servicio (*Directory Service Access*)
  - el uso de los privilegios otorgados a los usuarios (*Use of User Right*).
- 3) El servidor del Departamento de Matemáticas, configurado como *Primary Domain Controller (PDC)*, tenía 899 cuentas de acceso activas. El examen realizado sobre la configuración para el control de las contraseñas de dichas cuentas reveló que:
- a) Quince cuentas de acceso<sup>11</sup> pertenecientes a usuarios identificados como estudiantes graduados, profesores y personal administrativo no estaban configuradas para que expirara su contraseña en el sistema.
  - b) Una cuenta de acceso<sup>11</sup>, correspondiente a un exprofesor, permanecía activa en el sistema, luego de haber transcurrido más de siete meses desde que este se retiró.
  - c) En 505 cuentas<sup>11</sup> no se había definido un término fijo para que el sistema les requiriera a los usuarios la modificación de las contraseñas de sus cuentas. Dichas cuentas tenían marcada la opción *unknown*.

---

<sup>10</sup> Véase la nota al calce 9.

<sup>11</sup> Véase la nota al calce 5.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente, y de que la información sea accedida de forma no autorizada. Además, se establece que cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información. Estas normas se instrumentan, en parte, mediante lo siguiente:

- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos
- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente
- La renovación periódica de la contraseña de cada usuario, según las necesidades de la agencia y de los procedimientos establecidos.

En la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la *Carta Circular Núm. 77-05*, se establece que cada agencia será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso y las contraseñas, los controles de acceso al servidor y los sistemas para auditar el uso del sistema, la integridad y la seguridad de los datos y las comunicaciones enviadas.

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados, y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían a que el Coordinador de Servicios al Usuario I<sup>12</sup> del Departamento de Matemáticas y el Especialista en Telecomunicaciones I<sup>13</sup> del Departamento de IEC no habían puesto en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo, ni tenían un control adecuado sobre el mantenimiento de las cuentas de acceso.

En la carta del Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos y se atempere a la reglamentación. [sic]

#### **Hallazgo 4 - Contraseñas almacenadas sin estar cifradas**

- a. El examen de la seguridad de las contraseñas utilizadas para acceder el Sistema de Inventario de Propiedad y de las que se utilizaban para acceder de forma remota a un servidor<sup>14</sup> del Departamento de IEC, reveló que las mismas no se mantenían almacenadas en forma cifrada (*encrypted*<sup>15</sup>).

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas y directrices generales que permitirán a la agencia establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan.

En la Sección III, Políticas de Contraseñas, de las *Normas de Seguridad Lógica de los Sistemas Administrativos*, se establece, entre otras cosas, que las contraseñas no deben ser anotadas ni divulgadas a otra persona.

---

<sup>12</sup> Véase la nota al calce 7.

<sup>13</sup> Véase la nota al calce 8.

<sup>14</sup> Véase la nota al calce 9.

<sup>15</sup> Datos codificados que son ininteligibles para el lector.

La situación comentada propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados, y hacer uso indebido de esta. Además, propicia la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada se debía a que el Especialista en Telecomunicaciones I<sup>16</sup> del Departamento de IEC y el Registrador de Datos II<sup>17</sup> de la Oficina de Propiedad, no se aseguraron de mantener en forma cifrada las cuentas de acceso para proteger la divulgación y la lectura por otras personas.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos y se atempere a la reglamentación. [sic]

**Hallazgo 5 - Falta de almacenamiento de los respaldos en un lugar seguro fuera de los predios donde estaba ubicado el centro de computadoras del Departamento de IEC**

- a. Los respaldos (*backups*) correspondientes a los datos contenidos en tres servidores<sup>18</sup> ubicados en el centro de computadoras del Departamento de IEC, no se almacenaban en un lugar seguro, fuera de los predios de dicho Departamento.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que deberán existir procedimientos para tener y mantener una copia de respaldo recurrente, de la información y de los programas de aplicación y sistema esenciales e importantes para las operaciones de la agencia. En consonancia con dicha *Política* se requiere, entre otras cosas, que toda información almacenada en medios electrónicos, que se utilice como parte de

---

<sup>16</sup> Véase la nota al calce 8.

<sup>17</sup> Nombre del puesto que ocupaba el coordinador responsable de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicación en la Oficina de Propiedad.

<sup>18</sup> Véase la nota al calce 9.

la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre.

La situación comentada podría ocasionar la pérdida permanente de información importante, sin la posibilidad de poder recuperarla, lo que podría afectar adversamente las operaciones del Departamento de IEC.

La situación comentada se atribuye a que el Especialista en Telecomunicaciones I<sup>19</sup> del Departamento de IEC no había hecho las gestiones para mantener las copias de respaldo en un lugar seguro, fuera de los predios dicho Departamento.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos y se atempere a la reglamentación. [sic]

#### **Hallazgo 6 - Falta de normas y de procedimientos escritos, y procedimientos sin aprobar**

- a. No se habían promulgado normas ni procedimientos relacionados con la implantación, el desarrollo y el mantenimiento de los sistemas de información, y las redes de comunicaciones, según se indica:
  - 1) En los departamentos de Matemáticas y de IEC, no se habían promulgado normas ni procedimientos escritos para notificar a la persona encargada de la seguridad de los sistemas de información, el cese de usuarios por motivo de renuncia, separación o traslado. Esto, para cancelar la cuenta de acceso, local o remota, oportunamente al momento del cese del usuario de sus funciones.
  - 2) En la Oficina de Propiedad no se habían promulgado normas ni procedimientos escritos relacionados con la seguridad del Sistema de Inventario de Propiedad, ni con la asignación y eliminación de las cuentas de usuarios para acceder al mismo.

---

<sup>19</sup> Véase la nota al calce 8.

3) En el CTI no se habían preparado las normas ni los procedimientos necesarios para reglamentar los siguientes procesos relacionados con la administración, la seguridad y el uso de los sistemas computarizados:

- el control sobre los programas, las aplicaciones y las utilerías *open source*<sup>20</sup> que son descargados (*downloads*)
- la restricción de acceso a las aplicaciones del sistema operativo
- el uso y la revisión de los programas de utilerías
- la identificación, la selección, la instalación y la modificación del sistema operativo de las computadoras
- el control de los cambios de emergencia sobre la configuración de la aplicación del sistema operativo.

b. No se habían aprobado los siguientes procedimientos:

1) En el Departamento de Matemáticas no fueron aprobados por el Director los siguientes procedimientos:

- *Información sobre Seguridad*
- *Plan de Contingencias de Sistemas de Información*
- *Redes de Comunicación*

2) Los siguientes procedimientos no habían sido remitidos al Director del CTI para su revisión y aprobación:

- *Eliminación de Cuentas para ex funcionarios*

---

<sup>20</sup> Son programas de computadora disponibles en Internet libres de costo sin restricción de uso.

- *Seguridad en FRS*
- *Seguridad en HRS*

En el Inciso 6, Apartado C, de la Sección II de la *Política Computacional y de Comunicaciones del Recinto Universitario de Mayagüez*, se indica que decanatos, departamentos administrativos y académicos, laboratorios o cualquier otra unidad con recursos computacionales y de comunicación, podrán establecer normas y políticas aplicables a su unidad, siempre y cuando sean consistentes con la *Política Institucional* y con los *Procedimientos para el Uso Ético Legal de las Tecnologías de Información*.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente, sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer por escrito normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computarizadas y que estén aprobados por la alta gerencia. Mediante los mismos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuye a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilita la labor de adiestramiento.

Las situaciones comentadas podrían ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias.

Además, la situación comentada en el **apartado a.1)** propicia que las cuentas de exempleados y las del personal trasladado a otras áreas del RUM permanezcan activas en el sistema [Véase el Hallazgo 2-b.2b)(2) y 3-a.3b)], lo que podría causar que el mismo pueda ser accedido indebidamente.

Las situaciones comentadas en el **apartado a.1) y 2)** denotan que los directores departamentales y administrativos no velaron para que los encargados de sus respectivos centros de cómputos desarrollaran, para su consideración y aprobación, las normas y los procedimientos escritos para la notificación y la cancelación oportuna de las cuentas de acceso de los usuarios que hayan cesado de sus funciones.

La situación comentada en el **apartado a.3)** se atribuye a que el Coordinador de Servicios al Usuario I no remitió los procedimientos al Director del CTI para su revisión y aprobación.

La situación comentada en el **apartado b.1)** denota que el Director del CTI no veló ni requirió que se desarrollaran, para su consideración, las normas y los procedimientos escritos para reglamentar las operaciones mencionadas.

La situación comentada en el **apartado b.2)** se debió a que la Especialista en Sistemas Operativos II no remitió los procedimientos al Director del CTI para su revisión y aprobación.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos y se atempere a la reglamentación en lo que respecta a la actualización de las normas y procedimientos centrales (CTI), así también como en los departamentos académicos y administrativos y sus servidores. [sic]

**Hallazgo 7 - Deficiencias en los cuartos de distribución del cableado (*wiring closets*), y falta de actualización del diagrama esquemático de la red del RUM**

- a. El examen sobre la seguridad y el acceso físico existentes en 18 cuartos de distribución del cableado (*wiring closets*) en los que se mantenían los equipos de telecomunicaciones de la red del RUM, reveló lo siguiente:
- 1) Los equipos que se mantenían en el cuarto de distribución de cableado ubicado en el Edificio de Telefónica estaban expuestos a ser accedidos por personal no autorizado, según se indica:
    - La Oficina de Correo del RUM y el reloj ponchador para registrar la asistencia de los empleados que laboran en el Edificio de Telefónica estaban ubicados dentro del cuarto de distribución.
    - Los operadores del cuadro telefónico y los empleados del correo interno tenían acceso al cuarto de distribución.
    - En el cuarto de distribución se guardaban y se les daba carga a los carros eléctricos utilizados por los mensajeros. Además, se guardaban materiales de oficina, recipientes para recoger material reciclable de aluminio, plástico y vidrio, y equipos para la limpieza.
  - 2) En el examen realizado a los cuatro cuartos de distribución de cableado ubicados en el edificio del Departamento de IEC, se observaron las siguientes deficiencias:
    - a) El cuarto de distribución de cableado que tenía el enrutador principal del Departamento de IEC se utilizaba como almacén de equipo computadorizado.
    - b) Ninguno de los cuartos tenía diagramas esquemáticos de la infraestructura de la red por piso.

- c) En otro de los cuartos no se había identificado la cablería utilizada para la conexión entre los *hubs*<sup>21</sup> y los *switches*, lo cual es necesario para identificar cada cable y la estación de trabajo a la que corresponde.
  - d) Uno de los cuartos de distribución de cableado no contaba con un extintor de incendios. El extintor de incendios más cercano a dicho cuarto se mantenía dentro de un salón cerrado con llave.
- 3) En el examen realizado a los seis cuartos de distribución de cableado ubicados en el Departamento de Ingeniería Civil, se observaron las siguientes deficiencias:
- a) No había un extintor de incendios cerca de dos cuartos donde estaban instalados los equipos de telecomunicaciones y el enrutador principal del edificio de Ingeniería Civil.
  - b) Ninguno de los cuartos tenía diagramas esquemáticos de la infraestructura de la red por piso.
  - c) En dos de los cuartos no se había identificado la cablería utilizada para la conexión entre los *hubs* y los *switches*, lo cual es necesario para identificar cada cable y la estación de trabajo a la que corresponde.
  - d) El equipo de comunicaciones instalado en un salón<sup>22</sup> carecía de un gabinete con llave, por lo que estaba expuesto al acceso de los estudiantes y de los profesores.

---

<sup>21</sup> Dispositivo de comunicación que permite centralizar el cableado de una red. Se utiliza para ampliar una red y dividir el ancho de banda entre las estaciones de trabajo conectadas.

<sup>22</sup> La identificación del salón se incluyó en el borrador de los **hallazgos** de este *Informe*, remitido al entonces Rector y al ex Rector para comentarios.

- 4) En el examen realizado a seis cuartos de distribución de cableado donde se encontraba el equipo de telecomunicaciones del Departamento de Matemáticas, se observaron las siguientes deficiencias:
- a) No se había identificado la cablería utilizada para la conexión entre los *hubs* y los *switches*, lo cual es necesario para identificar cada cable y la estación de trabajo a la que corresponde.
  - b) No contaban con diagramas esquemáticos de la infraestructura de la red por piso.
  - c) Los cuartos de distribución de cableado ubicados en tres salones<sup>23</sup> no cumplían con las condiciones ambientales adecuadas para proteger el equipo de telecomunicaciones. Los referidos cuartos no tenían suficiente ventilación y estaban llenos de polvo. Además, en estos cuartos se almacenaban materiales como planchas de cielo raso.
  - d) Las paredes de un salón<sup>23</sup> donde se encontraban los equipos de telecomunicaciones no llegaban hasta el techo.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas y directrices generales que permitirán a la agencia establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Esto implica que, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- se controle adecuadamente el acceso de personas a dichas áreas
- no se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos

---

<sup>23</sup> Véase la nota al calce 22.

- se mantenga la documentación e identificación adecuada del cableado de conexión a la red, de forma que se puedan corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada
  - se utilice equipo y tecnología adecuada para proteger los sistemas
  - se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas.
- b. El examen del diagrama esquemático de la red de comunicaciones del RUM reveló que no había sido actualizado desde el 2006. El diagrama no presentaba 27 servidores que estaban ubicados en el Área de Operaciones del CTI. Además, en el mismo se incluía un servidor<sup>24</sup>, que al momento del examen no se encontraba en el CTI.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica* de la *Carta Circular Núm. 77-05*, se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implementar una infraestructura de Red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. Además, incluye como política que el diseño de la Red debe estar documentado.

Las mejores prácticas en el campo de la tecnología de información sugieren que, para mantener en funciones aceptables la red, es necesario establecer controles adecuados sobre los inventarios, la ubicación y las conexiones entre sus componentes. Esto se logra mediante la documentación detallada y actualizada de las conexiones que permita corregir a tiempo problemas de comunicación de la red y detectar cualquier conexión no autorizada.

Las situaciones comentadas en el **apartado a.1), 3)d) y 4)d)** pueden propiciar que personas ajenas a las operaciones de la red causen daños al equipo, por error o intención, lo que podría afectar adversamente el funcionamiento de la red y la continuidad de las operaciones del RUM.

---

<sup>24</sup> Véase la nota al calce 9.

Las situaciones que se comentan en el **apartado a.2)a) y 4)c)** pueden ocasionar daños y deterioros prematuros a los equipos de la red y a los equipos de computadoras, lo que dificulta obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos.

Las situaciones comentadas en el **apartado a.2)d) y 3)a)** pueden poner en riesgo la seguridad de los empleados y de los sistemas computadorizados. Además, podrían impedir la disponibilidad de los sistemas y, por consiguiente, limitar los servicios que prestan dichos departamentos.

Las situaciones comentadas en los **apartados a.2)b) y c), 3)b) y c), 4)a) y b), y b.** impedían al RUM controlar, administrar y efectuar un mantenimiento rápido, eficiente y efectivo de los equipos que componen su red. Además, impide resolver problemas de conexión en un tiempo razonable y efectuar una planificación efectiva para realizar mejoras a la red, según el crecimiento de sus sistemas.

La situación comentada en el **apartado a.1)** se debía, en parte, a que el Decano de Administración Interino no realizó las gestiones necesarias para aislar el área de Servicios Auxiliares del Área de Telecomunicaciones del Edificio Telefónica.

La situación comentada en el **apartado a.2)** se debía a que el Especialista en Telecomunicaciones I<sup>25</sup> no contaba con normas ni procedimientos escritos sobre la documentación y la seguridad que debían tener los cuartos de distribución de cableado que mantienen los equipos de telecomunicaciones del Departamento de IEC.

La situación comentada en el **apartado a.3)** se debía a que el Coordinador de Servicios Técnicos al Usuario I no contaba con normas ni procedimientos escritos sobre la documentación, la seguridad y el control de acceso físico que debían tener los cuartos de distribución de cableado que mantienen los equipos de telecomunicaciones del Departamento de Ingeniería Civil.

---

<sup>25</sup> Véase la nota al calce 8.

La situación comentada en el **apartado a.4)** se debía a que el Coordinador de Servicios al Usuario I<sup>26</sup> no contaba con normas ni procedimientos escritos sobre la documentación y la seguridad que debían tener los cuartos de distribución de cableado que mantienen los equipos de telecomunicaciones del Departamento de Matemática.

La situación comentada en el **apartado b.** se debía a que el Director del CTI solo mantenía un diagrama conceptual de la Red del RUM y que los detalles específicos se obtenían mediante herramientas computadorizadas que monitorean el comportamiento de la misma.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos y se atempere a la reglamentación en lo que respecta al CTI y departamentos académicos y administrativos. [sic]

**Hallazgo 8 - Limitaciones en la aplicabilidad de la *Guía RUMNET*, y falta de documentación de los análisis realizados a las actividades inusuales en los registros de la red, y de un itinerario para el mantenimiento de los equipos conectados a esta**

- a. El CTI contaba con la *Guía RUMNET* para reglamentar los procesos relacionados con la instalación, la configuración y la documentación de la red del RUM. Dicha *Guía* era utilizada como una interna del CTI y no era extensiva a las demás unidades institucionales o departamentos académicos del RUM, en donde se habían habilitado centros de cómputos.

En la *Guía RUMNET* se establece que el RUM, como parte de su infraestructura de instalaciones, posee una amplia red de comunicaciones de computadoras la cual abarca los 47 edificios que comprenden el Recinto y la estación remota de investigación Isla Maguelles. En este documento se presenta un descriptivo de la implantación de esta red y se establece una serie de guías para la administración, la operación y el crecimiento de la misma.

La situación comentada puede ocasionar que las instalaciones, las configuraciones y las inspecciones de la red del RUM, así como la documentación de estas, no se efectúen

---

<sup>26</sup> Véase la nota al calce 7.

uniformemente. Esto reduciría la eficacia y los controles de la misma, lo que expondría la información disponible a riesgos innecesarios. Además, afectaría la toma de decisiones al momento de modificar la red o algunos de sus componentes.

La situación comentada se debía a que el Director de CTI entendía que dicha *Guía* aplica principalmente a la red que el CTI administra directamente. Esta red se compone del *backbone* principal del RUM y de los equipos centrales de comunicaciones donde convergen todas las comunicaciones de los diferentes departamentos y edificios. Además, en la *Guía RUMNET* no se establecía un propósito ni un alcance con el fin de que fuera de aplicabilidad a todas las unidades del RUM que cuentan con un coordinador de informática responsable de implantar, desarrollar y mantener los sistemas de información computadorizados y las redes de comunicación en los diferentes departamentos.

- b. El Director de Servicios Técnicos y el Coordinador de Servicios al Usuario II del CTI eran los encargados de administrar la seguridad y el tráfico de la red. Estos no mantenían evidencia de haber efectuado y documentado los análisis de los datos recopilados mediante las herramientas de monitoreo a la red de las actividades inusuales o las fallas potenciales de seguridad.

Esta situación fue comentada en el informe *OAIC 2007-04* del 4 de mayo de 2007, emitido por la Oficina de Auditoría Interna de la Junta de Síndicos de la Universidad de Puerto Rico.

En la Sección 5.0 del *Manual de Procedimientos y Manejo de Firewalls*, aprobado en junio de 2007 por el Ayudante del Rector para Asuntos en Tecnología y Director del CTI, se establece, entre otras cosas, que a base de los análisis se determinará si hace falta hacer algún cambio en los *firewalls*, o reaccionar ante una amenaza a la red o a los sistemas. Los incidentes más significativos serán documentados. Además, se establece que aquellos incidentes que provengan de redes externas, se documentarán y se monitorearán para controlar su efecto.

La situación comentada dificulta identificar oportunamente patrones de amenazas y ataques al sistema, y fallas en su configuración. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

La situación comentada obedece, principalmente, a que el Ayudante del Rector para Asuntos en Tecnología y Director del CTI consideraba que no era práctico documentar los análisis realizados sobre las actividades inusuales identificadas en los registros de tráfico de la red, debido al excesivo volumen de los mismos.

- c. El CTI no mantenía un itinerario para efectuar el mantenimiento preventivo de los equipos principales conectados a la red.

En la *Política Núm. TIG-004, Servicios de Tecnología* de la *Carta Circular Núm. 77-05* se establece que el personal de la oficina de tecnología de información de la agencia será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos. Además, revisará regularmente sus sistemas para verificar que funcionen adecuadamente.

La situación comentada podría propiciar que fallas en dichos equipos no sean detectadas a tiempo. Esto, a su vez, puede resultar en una falla mayor en el sistema que interrumpa las operaciones del CTI y, por ende, los servicios que este presta a sus usuarios.

Esta situación se debía a que el Director de Servicios Técnicos realizaba el mantenimiento preventivo de los equipos cuando surgía la oportunidad, por lo que no programaba el ofrecimiento del mismo.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos sobre la *Guía RUMNET* del CTI, la administración de la seguridad y el tráfico de la red del CTI, y sobre el itinerario de mantenimiento preventivo de los equipos en el CTI, adoptándose de esa manera a la reglamentación. [sic]

### **Hallazgo 9 - Falta de un registro de los servidores autorizados a ser instalados en la red del RUM, y de problemas ocurridos en los sistema operativos**

- a. En el CTI no se mantenía un registro de los servidores autorizados a ser instalados en la red del RUM.

En la Sección 2.5 de la *Guía RUMNET* se establece, entre otras cosas, que todo servidor debe ser registrado antes de su implementación. El Registro del Servidor debe incluir la siguiente información: nombre del servidor, sistema operativo, ubicación, propósito, departamento, nombre del administrador, teléfono del administrador, servicios que brindará y usuarios del sistema (local, intranet, Internet). Todo registro de servidor deberá ser autorizado por el Coordinador de Tecnologías y el Administrador de Red del RUM. Solamente los servidores debidamente registrados serán autorizados a transmitir y recibir comunicación de la red del RUM.

La situación comentada priva al CTI de mantener un control sobre los servidores debidamente autorizados a transmitir y recibir comunicación en la red del RUM y de la información necesaria para la identificación oportuna de algún servidor con problemas, que permita tomar de inmediato las acciones preventivas y correctivas necesarias.

La situación comentada se atribuye a que el Director de Servicios Técnicos entendía que se mantenía un control de los servidores a través del enrutador del RUM, donde se documenta el nombre del servidor, el *ip address*<sup>27</sup>, la ubicación y, en algunos casos, el nombre de la persona encargada y otra información relevante.

- b. El Coordinador de Servicios Técnicos al Usuario II no mantenía un registro para identificar y documentar los problemas ocurridos en los sistemas operativos de los servidores, y cómo los mismos fueron resueltos. Esto, para que en caso de que se repita algún problema se pueda hacer referencia a la solución.

---

<sup>27</sup> Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345.

Las mejores prácticas en el campo de la tecnología para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que se debe mantener un registro estandarizado en el cual se anoten los problemas con los sistemas, y cómo fueron resueltos. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado.

La situación comentada podría propiciar la improvisación, y que en casos de emergencia se tomen medidas inapropiadas y en forma desordenada. Esto afectaría el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información en un tiempo razonable.

La situación comentada se debió a que el Coordinador de Servicios Técnico II no había considerado la importancia de mantener este registro.

En la carta del entonces Rector, este nos indicó lo siguiente:

Se impartirán instrucciones y tomarán medidas correctivas para que se corrijan los señalamientos sobre el registro de servidores en la red del RUM por CTI y el registro de novedades del sistema operativo de los servidores en la red del RUM por CTI, adoptándose de esa manera a la reglamentación. [sic]

**ANEJO 1**

UNIVERSIDAD DE PUERTO RICO  
RECINTO UNIVERSITARIOS DE MAYAGÜEZ  
CENTRO DE TECNOLOGÍA DE INFORMACIÓN  
**MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS  
QUE ACTUARON DURANTE EL PERÍODO AUDITADO**

<b>NOMBRE</b>	<b>CARGO O PUESTO</b>	<b>PERÍODO</b>	
		<b>DESDE</b>	<b>HASTA</b>
Ing. Carlos H. del Río Rodríguez	Presidente	14 oct. 08	20 mar. 09
Lcdo. Salvador Antonetti Zequeira	Secretario	14 oct. 08	20 mar. 09

**ANEJO 2**

UNIVERSIDAD DE PUERTO RICO  
RECINTO UNIVERSITARIOS DE MAYAGÜEZ  
CENTRO DE TECNOLOGÍA DE INFORMACIÓN  
**FUNCIONARIOS PRINCIPALES QUE ACTUARON  
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Jorge Iván Vélez Arocho	Rector	14 oct. 08	20 mar. 09
Ing. Víctor Díaz Rodríguez	Ayudante del Rector para Asuntos en Tecnología y Director del Centro de Tecnología de Información	14 oct. 08	20 mar. 09
Dr. José A. Frontera Agenjo	Decano de Administración Interino	14 oct. 08	20 mar. 09
Dr. Moisés Oregón Avilés	Decano del Colegio de Artes y Ciencias	14 oct. 08	20 mar. 09
Dr. Ramón Vázquez Espinosa	Decano del Departamento de Ingeniería	14 oct. 08	20 mar. 09
Dr. Isidoro Couvertier Reyes	Director del Departamento de Ingeniería Eléctrica y Computadoras	14 oct. 08	20 mar. 09
Dr. Ismael Pagán Trinidad	Director del Departamento de Ingeniería Civil	14 oct. 08	20 mar. 09
Dr. Julio C. Quintana Díaz	Director del Departamento de Matemáticas	14 oct. 08	20 mar. 09