



*Secretaría*

**MANUEL A. TORRES NIEVES**  
*Manuel A. Torres Nieves*  
SECRETARIO DE SENADO

- 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

---

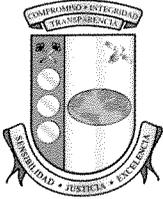
- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

### 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

10227



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

RECIBIDO SECRETARIA  
SECRETARIA P.R.

2012 JUN 10 AM 9:34

Yesmín M. Valdivieso

Contralora

17 de enero de 2012

**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-12-05* de la Oficina de Sistemas de Información de la Universidad de Puerto Rico en Cayey aprobado por esta Oficina el 15 de diciembre 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*  
Yesmín M. Valdivieso

Anejo

RECIBIDO  
SECRETARIA P.R.  
THOMAS RIVERA SCHATZ  
2012 JUN 17 PM 2:12

10227



**INFORME DE AUDITORÍA TI-12-05**

15 de diciembre de 2011

**Universidad de Puerto Rico en Cayey**

**Oficina de Sistemas de Información**

(Unidad 5495 - Auditoría 13189)

Período auditado: 23 de julio de 2008 al 17 de julio de 2009



## 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>7</b>
<b>COMENTARIO ESPECIAL.....</b>	<b>7</b>
Cuentas de correo electrónico con contraseñas que no estaban en formato cifrado .....	7
<b>INFORME DE AUDITORÍA ANTERIOR.....</b>	<b>8</b>
<b>RECOMENDACIONES .....</b>	<b>9</b>
A LA JUNTA DE SÍNDICOS DE LA UNIVERSIDAD DE PUERTO RICO .....	9
AL PRESIDENTE DE LA UNIVERSIDAD DE PUERTO RICO.....	9
AL RECTOR DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY.....	9
<b>CARTAS A LA GERENCIA.....</b>	<b>12</b>
<b>COMENTARIOS DE LA GERENCIA .....</b>	<b>12</b>
<b>AGRADECIMIENTO.....</b>	<b>13</b>
<b>RELACIÓN DETALLADA DE HALLAZGOS.....</b>	<b>14</b>
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	14
HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY .....	15
1 - Falta de un informe de avalúo de riesgos sobre los sistemas de información computadorizados .....	15
2 - Deficiencias en los parámetros de seguridad de los servidores y en el proceso de eliminar las cuentas de acceso de los exempleados.....	17

- 3 - Falta de almacenamiento de los respaldos y de la documentación de los sistemas y las aplicaciones en un lugar seguro fuera de la UPR-Cayey, y deficiencias relacionadas con el acuerdo para mantener un centro alternativo de recuperación de los sistemas de información ..... 19
- 4 - Deficiencias relacionadas con los procedimientos y con las normas sobre los sistemas de información, y falta de procedimientos escritos para la eliminación de información y de programas ..... 23
- 5 - Falta de controles físicos y ambientales en los cuartos de distribución de cableado, y deficiencias relacionadas con el diagrama esquemático de la red.... 26
- 6 - Falta de adiestramientos al personal de la OSI a cargo de la seguridad y de administrar la red ..... 31
- 7 - Falta de controles sobre los equipos de la red y deficiencias en su mantenimiento ..... 33
- ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS QUE ACTUARON DURANTE EL PERÍODO AUDITADO ..... 36**
- ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO ..... 37**

Informe de Auditoría TI-12-05  
15 de diciembre de 2011  
Unidad 5495 - Auditoría 13189

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

15 de diciembre de 2011

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Universidad de Puerto Rico en Cayey (UPR-Cayey) 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.

### **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.

La UPR-Cayey inició sus actividades académicas en el 1967. La misma fue creada por autorización del Consejo de Educación Superior (Consejo). En los primeros años operó como Colegio Regional y ofrecía oportunidades de educación de dos años a nivel universitario.

Mediante la *Certificación Núm. 37* del 19 de diciembre de 1969, el Consejo extendió los ofrecimientos educativos del Colegio a cuatro años, de forma tal, que se otorgaran grados de bachillerato. En esa misma fecha fue separado de la Administración de Colegios Regionales y se convirtió en el Colegio Universitario de Cayey, bajo la supervisión directa del Presidente de la Universidad.

Mediante la *Certificación Núm. 117* del 2 de abril de 1982, el Consejo concedió autonomía al Colegio dentro del Sistema Universitario. El poder nominador, que hasta esta fecha lo tenía el Presidente de la Universidad, le fue transferido al Director y Decano del Colegio. Además, se crearon la Junta Administrativa y la Junta Académica del Colegio, las cuales estarían presididas por el Director y Decano del Colegio. Mediante la *Certificación Núm. 144* del 29 de abril de 1983 el Consejo le cambió el título al puesto de Director y Decano del Colegio por el de Rector.

La administración y supervisión de las operaciones de la UPR-Cayey las ejerce un Rector nominado por el Presidente de la Universidad, previa consulta de este al Senado Académico, para ser nombrado por la Junta de Síndicos. Las áreas operacionales se administran mediante los decanatos de Asuntos Administrativos, Asuntos Académicos y Asuntos Estudiantiles.

El 1 de agosto de 2007, el Rector Interino consolidó la Oficina de Tecnologías de Información (OTI), la Oficina de Tecnologías para la Docencia (OTD) y el Área de Televisión Educativa en una sola oficina conocida como la OSI. Esta es dirigida por un Director de Sistemas de Información y está adscrita a la Oficina del Rector. La OSI cuenta con 1 Director de Tecnología Académica y Administrativa, 1 Director de Desarrollo de Tecnologías de Información, 1 Supervisor de Operadores de Computadores Electrónicos, 3 especialistas en tecnologías de información II, 1 Operador de Computador Electrónico I, 1 Operador de Computador Electrónico II, 1 Coordinador de Servicios Técnicos al Usuario I, 1 Especialista de Equipo Computadorizado y Telecomunicaciones II, 1 Analista de Programas de Sistemas Electrónicos II y 1 Secretaria Administrativa V.

Los recursos para los gastos de funcionamiento de la UPR-Cayey provienen de asignaciones legislativas, fondos federales, donativos, e ingresos propios. Para el año fiscal 2007-08, el presupuesto asignado a la UPR-Cayey y a la OSI fue de \$122,583,549 y de \$1,611,504, respectivamente.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta de Síndicos y de los funcionarios principales de la UPR-Cayey, respectivamente, que actuaron durante el período auditado.

La UPR-Cayey cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.cayey.upr.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 23 de julio de 2008 al 17 de julio de 2009. En algunos aspectos examinamos transacciones de fechas anteriores. 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

La pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a los controles relacionados con la administración del programa de seguridad, el acceso lógico a los sistemas de información computadorizados, la continuidad del servicio y la red de comunicaciones, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 7**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

## COMENTARIO ESPECIAL

En esta sección se comentan situaciones que no necesariamente impliquen violaciones de leyes y reglamentos, pero que sean significativas para las operaciones de la unidad auditada. Por ejemplo: litigios o demandas pendientes y pérdidas en las operaciones de la entidad. También se incluyen situaciones que no están directamente relacionadas con las operaciones de la entidad, las cuales pueden constituir violaciones de ley y de reglamento, que afectan al erario.

### **Cuentas de correo electrónico con contraseñas que no estaban en formato cifrado<sup>1</sup>**

El Sistema de la Universidad de Puerto Rico (UPR) impulsó un proyecto para las cuentas de correo electrónico que utilizaban los estudiantes, y el personal docente y no docente dentro del marco de su plan estratégico *Diez para la década*. Dicho proyecto consistió en la creación de cuentas de correo electrónico a través de la plataforma *Google Applications for Education (GAE)*. El proyecto se le conoció como *UPR-GAE*. El examen del informe de las cuentas de los usuarios de la UPR-Cayey extraído del directorio *OpenLDAP* del sistema de correo

---

<sup>1</sup> Técnica que se utiliza para proteger el texto normal, que codifica los datos para que no sean legibles.

electrónico *UPR-GAE* el 18 de mayo de 2009, reveló que 1,038 de 7,114 cuentas no tenían las contraseñas en formato cifrado. Por esto, las mismas se podían leer. Estas cuentas se desglosaban de la siguiente manera:

USUARIOS	CANTIDAD DE CUENTAS	CUENTAS CON CONTRASEÑAS NO CIFRADAS	POR CIENTO CUENTAS NO CIFRADAS
Estudiantes	6,541	870	13
Empleados no docentes	310	100	32
Empleados docentes	<u>263</u>	<u>68</u>	26
Total	<u>7,114</u>	<u>1,038</u>	

Las mejores prácticas utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que las contraseñas deben estar internamente cifradas sin posibilidad de descifrado, y no deben ser visibles en ninguna forma. Esto, para reducir el riesgo de que una persona no autorizada obtenga acceso a los sistemas de información.

La situación comentada pone en riesgo la seguridad, la confidencialidad y la integridad de la información transmitida a través de correo electrónico, al permitir que las cuentas de los usuarios puedan ser utilizadas por personas no autorizadas para acceder a este, con la intención de hacer daño o alterar la información del sistema sin que se puedan fijar responsabilidades.

### INFORME DE AUDITORÍA ANTERIOR

Una situación similar a la comentada en el **Hallazgo 7-a.1)** de este *Informe* fue objeto de recomendaciones en el *Informe de Auditoría CPED-92-10* del 30 de junio de 1992. Estas no fueron atendidas.

El no atender, sin justa causa, las recomendaciones de los informes de auditoría de esta Oficina puede constituir una violación al Artículo 3.2(b) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, según enmendada. A estos efectos, el 30 de enero de 1987, el Director Ejecutivo de la Oficina de

Ética Gubernamental de Puerto Rico emitió la *Carta Circular Núm. 86-4*, mediante la cual exhortó a los alcaldes y a los funcionarios de la Rama Ejecutiva del Gobierno a cumplir con las mismas.

## 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 las **recomendaciones 2 y 3** de este *Informe*. [**Hallazgos del 1 al 7**]

### AL PRESIDENTE DE LA UNIVERSIDAD DE PUERTO RICO

2. Tomar las medidas necesarias para asegurarse de que la situación comentada en el **Comentario Especial** se corrija y no se repita.
3. Ver que el Rector de la UPR-Cayey cumpla con las **recomendaciones de la 4 a la 10** de este *Informe*. [**Comentario Especial y hallazgos del 1 al 7**]

### AL RECTOR DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY

4. Informar a los encargados del proyecto del sistema *UPR-GAE* a nivel de la Administración Central de la Universidad de Puerto Rico, la falla relacionada con las contraseñas utilizadas para acceder dicho sistema, para que tomen prontamente las medidas correctivas que correspondan. [**Comentario Especial**]
5. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece 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, Equipos 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, y se sugieren en las mejores prácticas en el campo de la tecnología. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. [**Hallazgo 1**]

6. Ejercer una supervisión efectiva sobre el Director de la OSI para asegurarse de que:
  - a. Supervise las funciones del Especialista en Equipos de Computadoras y Telecomunicaciones II, para que:
    - 1) Restrinja el horario de acceso a los recursos de la red, según las funciones y las responsabilidades de los usuarios. **[Hallazgo 2-a.]**
    - 2) Elimine prontamente las cuentas de acceso de los empleados que hayan cesado sus funciones en la UPR-Cayey y vea que, en lo sucesivo, las cuentas se eliminen en el momento en que el empleado cesa. Esto, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 2-b.**
  - b. Mantenga una copia de la documentación de los sistemas y de las aplicaciones en un lugar seguro fuera de los predios de la UPR-Cayey. **[Hallazgo 3-b.]**
  - c. Solicite a su personal que desarrolle, actualice y remita, para la aprobación del Rector, las normas y los procedimientos indicados en el **Hallazgo 4-a.1) y b.**
  - d. Remita para su consideración y aprobación las normas y los procedimientos indicados en el **Hallazgo 4-a.2).**
  - e. Establezca las medidas necesarias para corregir las situaciones indicadas en el **Hallazgo 5-a.** Esto, de manera que se asegure de que los equipos de comunicación se mantengan en lugares donde estén debidamente protegidos contra accesos no autorizados y contra posibles daños causados por condiciones físicas y ambientales, que puedan afectar la confidencialidad de la información, y la disponibilidad y el rendimiento de estos equipos.
  - f. Incluya la información que se comenta en el **Hallazgo 5-b.** en la documentación de la configuración de la red.
  - g. Identifique las necesidades de adiestramiento del personal de la OSI y, en coordinación con la Directora de la Oficina de Recursos Humanos, establezcan un

- plan anual de adiestramientos. Este plan debe contar con los temas identificados en el estudio de necesidades de adiestramiento, las nuevas tendencias en el área de seguridad y tecnología, así como la frecuencia con la que se ofrecerán los mismos, las horas mínimas requeridas a cada uno de los participantes y la inherencia de los temas con sus funciones. Además, vea que se cumpla con dicho plan y que se mantenga evidencia de los adiestramientos e información con los nombres de los participantes y las fechas en que se ofrecieron. **[Hallazgo 6]**
- h. Imparta instrucciones al personal a cargo de la red para que cuando instale equipos que no estén numerados, notifique al personal de la Oficina de Propiedad para que identifique y numere el mismo. **[Hallazgo 7-a.1]**
  - i. Revise el borrador del *Plan de Reposición, Actualización y Mantenimiento de Equipos y Software*, e incluya una disposición que establezca un itinerario para el mantenimiento preventivo de los equipos computadorizados, y requiera que se mantenga un registro o la documentación relacionada con los servicios de mantenimiento ofrecidos a los mismos, y lo remita para su aprobación. Una vez aprobado, asegurarse de que se cumpla con este. **[Hallazgo 7-b.]**
7. Ver que la Directora de la Oficina de Recursos Humanos, en coordinación con el Director de la OSI, establezca un procedimiento para que se notifique a tiempo a la OSI el cese de un usuario en sus funciones, para la cancelación de la cuenta de acceso de este. **[Hallazgo 2-b.]**
8. Realizar las gestiones pertinentes para asignar los recursos necesarios para que el personal de la OSI pueda mantener los respaldos de información de los servidores en un lugar seguro fuera de los predios de la UPR-Cayey. **[Hallazgo 3-a.]**
9. Enmendar los acuerdos recíprocos para restaurar las operaciones en caso de emergencia, para que en estos se incluyan todos los elementos descritos en el **Hallazgo 3-c.**

10. Ejercer una supervisión efectiva sobre la Oficial de Propiedad para asegurarse de que esta:
  - a. Imparta instrucciones a su personal para que identifique y numere los equipos mencionados en el **Hallazgo 7-a.1).**
  - b. Actualice el inventario de propiedad para que incluya los equipos mencionados en el **Hallazgo 7-a.2).**

### CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos 1 y 6**, incluidos en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**, se remitieron al Dr. Ram S. Lamba Bhiranwawali, entonces Rector de la UPR-Cayey, mediante carta de nuestros auditores del 3 de agosto de 2009.

El borrador de los **hallazgos** de este *Informe* se remitió al Dr. Juan N. Varona Echeandía, Rector de la UPR-Cayey, para comentarios mediante carta del 1 de abril de 2011. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al doctor Lamba Bhiranwawali, ex-Rector, mediante carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por la UPR-Cayey.

### COMENTARIOS DE LA GERENCIA

El 17 de agosto de 2009, el doctor Lamba Bhiranwawali, remitió sus comentarios sobre los **hallazgos 1 y 6** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El 5 de abril de 2011 el Rector y el ex-Rector solicitaron prórroga hasta el 30 de abril de 2011 para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 6 y 7 de abril de 2011, le concedimos las prórrogas solicitadas al ex-Rector y al Rector, respectivamente, hasta el 30 de abril de 2011. El Rector y el ex-Rector remitieron sus

Informe de Auditoría TI-12-05  
15 de diciembre de 2011  
Unidad 5495 - Auditoría 13189

comentarios al borrador de los **hallazgos** de este *Informe* mediante cartas del 29 de abril de 2011<sup>2</sup>. Los comentarios de dichos funcionarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la segunda parte de este *Informe*, titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY.

### AGRADECIMIENTO

A los funcionarios y a los empleados de la UPR-Cayey, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Por:

*Oficina del Central  
Jesús M. Valderrama*

---

<sup>2</sup> El Rector y ex-Rector emitieron cartas individuales que incluían los mismos comentarios para las situaciones comentadas en los **hallazgos**.

## 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 LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY, 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 LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE PUERTO RICO EN CAYEY

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

### **Hallazgo 1 - Falta de un informe de avalúo de riesgos sobre los sistemas de información computadorizados**

a. Un avalúo de riesgos es un método para identificar las vulnerabilidades y las amenazas a los recursos de sistemas de información. Además, evalúa los posibles daños para determinar dónde implantar las medidas de seguridad para poder alcanzar y cumplir con los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 20 de agosto de 2008, en la UPR-Cayey no se había realizado un avalúo de riesgos sobre los sistemas de información computadorizados.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada agencia deberá 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. Para esto deberá llevar a cabo un análisis de riesgos que incluya:

- Un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.
- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido, entre otras) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

La situación comentada impide a la UPR-Cayey evaluar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información. Además, impide el desarrollo de un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones de la UPR-Cayey, en caso de que surja alguna eventualidad.

La situación comentada se atribuye a que el Rector no había promulgado una directriz para la preparación y la documentación del avalúo de riesgos de los sistemas de información de la UPR-Cayey, según lo establecido en la *Carta Circular Núm. 77-05*.

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

Se va a implementar un Plan de Avalúo de Riesgo sobre los Sistemas de Información Computarizados en UPR Cayey y el mismo estará dirigido a identificar las vulnerabilidades y las amenazas que puedan ocurrir. Para ello se tomaran en consideración los criterios establecidos por la Oficina del Contralor.  
[sic]

**Hallazgo 2 - Deficiencias en los parámetros de seguridad de los servidores y en el proceso de eliminar las cuentas de acceso de los exempleados**

- a. El examen efectuado el 3 de abril de 2009, sobre los parámetros de seguridad relacionados con las cuentas de acceso establecidos en los cuatro servidores<sup>3</sup> configurados como *Domain Controller*, reveló que no se había restringido el tiempo de acceso a la red para todas las cuentas de acceso de acuerdo con las funciones de cada usuario. El sistema les permitía a los usuarios tener acceso los 7 días de la semana y las 24 horas del día.
- b. Al 4 de marzo de 2009, no se habían eliminado las cuentas de acceso de 20 empleados<sup>4</sup> que cesaron sus funciones entre el 31 de agosto de 2005 y el 31 de diciembre de 2008.

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. También se establece que cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de manera que estas circunstancias no afecten la seguridad de la información ni de los

---

<sup>3</sup> Los nombres de los servidores se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector y al ex-Rector de la UPR-Cayey para comentarios.

<sup>4</sup> Una relación de los nombres de los empleados se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector y al ex-Rector de la UPR-Cayey para comentarios.

sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre la Oficina de Recursos Humanos, el área en que trabaja el empleado y la OSI. Esta norma se constituye, 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 por motivo de renuncia, separación o traslado, para la cancelación de su cuenta de acceso.

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas de información 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 detectadas a tiempo para fijar responsabilidades.

La situación comentada en el **apartado a.** se debía a que el Especialista en Equipos de Computadoras y Telecomunicaciones II, quien fungía como Administrador de Seguridad, no había puesto en vigor todas las opciones de seguridad de acceso lógico que provee el sistema operativo, ni mantenía un control adecuado sobre el mantenimiento de las cuentas de acceso a la red.

La situación comentada en el **apartado b.** se debía a que no existían procedimientos escritos que les requirieran a los empleados de la Oficina de Recursos Humanos informarle al personal de la OSI el cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para proceder con la cancelación de su cuenta de acceso.

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

Se va a establecer a nivel del Rector y el "Staff" procedimientos de qué personal y/u oficina tendrá acceso a sus estaciones de trabajo fuera de horas laborables o días laborables. [sic] [**Apartado a.**]

Al momento de trabajar este borrador se desactivaron las cuentas de acceso de los 20 empleados que se mencionan. Además, el Director de OSI dio instrucciones al especialista a cargo de las cuentas de acceso a verificar, en coordinación con la oficina de recursos Humanos, qué personal, docente y no docente, no está activo en la Institución para desactivar la cuenta. [sic] [Apartado b.]

**Hallazgo 3 - Falta de almacenamiento de los respaldos y de la documentación de los sistemas y las aplicaciones en un lugar seguro fuera de la UPR-Cayey, y deficiencias relacionadas con el acuerdo para mantener un centro alternativo de recuperación de los sistemas de información**

- a. La UPR-Cayey contaba con un centro de respaldo externo. Dos veces al mes, personal de este centro recogía las cintas en la UPR-Cayey y las almacenaban en sus instalaciones. El examen realizado el 1 de junio de 2009, reveló que los respaldos<sup>5</sup> correspondientes a los archivos de la configuración de los usuarios contenidos en 26 servidores, no se almacenaban en el centro de respaldo externo de la UPR-Cayey.

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 (*backup*) recurrente de la información y de los programas de aplicación y de sistema esenciales e importantes para las operaciones de la agencia. En consonancia con dicha política pública es necesario, entre otras cosas, que toda información almacenada en medios electrónicos, que se utilice como parte de 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 afectaría adversamente las operaciones de la UPR-Cayey.

La situación comentada se debía a que el personal de la OSI tenía pocas cintas magnéticas para los respaldos y las reutilizaba, ya que las mismas tenían un alto costo y no contaban

---

<sup>5</sup> Los nombres de los respaldos se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector y al ex-Rector de la UPR-Cayey para comentarios.

con el presupuesto para la compra de unidades adicionales. Además, este personal consideraba que el mantener estas cintas le causaría un problema de almacenamiento, ya que cada respaldo requiere alrededor de tres cintas.

- b. La UPR-Cayey no mantenía copias de la documentación de los sistemas ni de las aplicaciones en el centro de respaldo externo.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan copias actualizadas de los manuales de operación de los sistemas de información, y de la documentación de las aplicaciones y de los programas en un lugar seguro fuera del edificio donde radica el centro. Esto es necesario para garantizar la continuidad de las operaciones en caso de que ocurra un evento inesperado en las instalaciones de la UPR-Cayey.

La situación comentada podría afectar la continuidad de las operaciones de la OSI si ocurriera alguna eventualidad que afectara las instalaciones de esta y destruyera toda la documentación y los manuales que allí se almacenan. Además, de ocurrir una emergencia que impida el acceso a la UPR-Cayey, el personal de la OSI no tendría acceso a toda la documentación necesaria para iniciar el proceso de reconstrucción de archivos y programas, y para el restablecimiento y la continuidad de las operaciones de los sistemas de información, en un tiempo razonable.

La situación comentada se debía a que la Directora Interina de la OSI no había requerido que se mantuviera copia de la documentación relacionada con las configuraciones del sistema computadorizado y de las aplicaciones y los programas utilizados, en un lugar seguro fuera de los predios de la UPR-Cayey.

- c. Mediante cartas del 6 y 7 de noviembre de 2008, la Vicepresidenta en Investigación y Tecnología de la Administración Central de la Universidad de Puerto Rico y el Rector de la

UPR-Cayey, respectivamente, formalizaron acuerdos recíprocos para restaurar las operaciones computadorizadas en caso de emergencia. Nuestro examen de dichos acuerdos reveló que los mismos no proveían para:

- Identificar las situaciones consideradas como emergencia y los arreglos correspondientes permitidos.
- Establecer el tipo de centro requerido, tal como: un centro totalmente equipado y listo para servicio de respaldo inmediato (*hot site*) o un centro no equipado que requeriría cierto tiempo para prepararlo para operaciones (*cold site*).
- Identificar los servicios o arreglos con proveedores de equipo de computadoras, de servicios de telecomunicaciones, de formularios y otros suministros de oficina.
- Identificar las operaciones críticas que serán restauradas en el centro alternativo.
- Coordinar la prioridad de procesamiento que tendrán las operaciones críticas de la entidad sobre las de otras entidades que necesiten utilizar el centro alternativo a la misma vez.
- Inspeccionar el centro alternativo y efectuar las verificaciones de capacidad y compatibilidad del equipo.
- Realizar los simulacros o las pruebas en el centro alternativo, por lo menos, una vez al año.
- Coordinar los arreglos de viaje y estadía del personal de la UPR-Cayey que trabaje en el centro alternativo, de ser necesario.
- Revisar periódicamente los términos del acuerdo para determinar si son adecuados para satisfacer las necesidades de la UPR-Cayey.

Las mejores prácticas utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte integral del plan de continuidad de negocios, se formalicen convenios con otras entidades

que posean equipos y sistemas de información compatibles que faciliten restaurar prontamente las operaciones computadorizadas, en caso de desastre o de otro tipo de emergencia que afecte las mismas. En dichos convenios se deben estipular, entre otras cosas, las necesidades y los servicios requeridos para afrontar una emergencia y los lugares donde podrían ser requeridos dichos servicios.

La situación mencionada podría afectar las funciones de la UPR-Cayey y los servicios de la OSI, ya que no tendrían establecidas las directrices escritas a seguir para implantar el plan de contingencias en el centro alterno. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la OSI.

La situación comentada se atribuye a que el Rector de la UPR-Cayey no se aseguró de que los acuerdos formalizados incluyeran los elementos necesarios para asegurar que la OSI pueda restaurar sus operaciones computadorizadas en las instalaciones de la Administración Central de la Universidad de Puerto Rico, en caso de una emergencia.

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

En la actualidad este sistema de resguardo no se está utilizando debido a que se encuentra con problemas de acceso a las bases de datos, servidores [...], servidores virtuales y toma mucho tiempo para finalizar el proceso. En estos momentos se están utilizando discos o espacios en otros servidores provisionalmente ya que estamos en proceso de adquirir nuevos servidores y además el nuevo sistema de resguardo el cual cumple con todas las necesidades. [sic] **[Apartado a.]**

Con la adquisición del nuevo sistema de resguardo la documentación de los sistemas se incluirán en el procedimiento, y por otra parte, producirá el acuerdo a nivel de servicio para la restauración del sistema en el lugar alterno, que en nuestro caso es en [...]. [sic] **[Apartado b.]**

**Hallazgo 4 - Deficiencias relacionadas con los procedimientos y con las normas sobre los sistemas de información, y falta de procedimientos escritos para la eliminación de información y de programas**

a. Al 22 de junio de 2009, la OSI contaba con los siguientes procedimientos y normas para regir las operaciones de sus sistemas de información:

- *Procedimiento para Instalar Computadoras*
- *Procedimiento para el Restablecimiento de sus Sistemas de Información en Caso de Desastre*
- *Normas para la Conexión de Servidores, Segmentos de Redes Locales y Nodos a CUCNET, revisado el 30 de agosto de 2000*
- *Normas Internas de Seguridad de la Oficina de Sistemas de Información.*

El examen realizado a estos procedimientos y normas reveló las siguientes deficiencias:

- 1) No consideraban aspectos relacionados con el rendimiento de los recursos de la red de comunicación y con el mantenimiento de los equipos conectados a esta, ni las especificaciones de los equipos y accesorios de conexión.
- 2) El *Procedimiento para Instalar Computadoras* y las *Normas para la Conexión de Servidores, Segmentos de Redes Locales y Nodos a CUCNET* no habían sido remitidos al Rector para su aprobación.

En la Sección 18.2 del *Reglamento General de la Universidad de Puerto Rico* del 16 de febrero de 2002, según enmendado, aprobado por la Junta de Síndicos, se establece que cada rector o director de unidad institucional emitirá las instrucciones administrativas necesarias para el buen funcionamiento interno de su unidad.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establecen las directrices generales que permiten a las agencias establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la

disponibilidad de la información que manejan. Será responsabilidad de cada entidad gubernamental desarrollar políticas específicas de seguridad y tomar en cuenta 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 computadorizadas y que estén aprobadas por la alta gerencia. Mediante las mismas 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, podría exponer al personal, a los equipos y a la información de la UPR-Cayey a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

La situación comentada en el **apartado a.1)** se atribuye a que la Directora Interina de la OSI no veló que su equipo de trabajo desarrollara y actualizara las normas y los procedimientos escritos de manera específica para atemperarlos con las operaciones de la red de comunicación de la UPR-Cayey.

La situación comentada en el **apartado a.2)** se debía a que la Directora Interina de la OSI no había cumplido con su deber de remitir los mencionados procedimientos y normas al Rector para su consideración y aprobación.

- b. Al 8 de julio de 2009, no se habían promulgado procedimientos escritos para eliminar la información confidencial y los programas archivados en los equipos computadorizados y en los medios de almacenamiento electrónico, antes de transferir o descartar los mismos.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que cuando las entidades gubernamentales vayan a disponer de equipo que contiene información sensible deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las instalaciones de la agencia. Además, en la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de dicha *Carta Circular*, se establece que cada agencia deberá establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y de las herramientas de trabajo que estos proveen. Esto implica que, como norma de sana administración, se adopten procedimientos escritos para eliminar la información confidencial y los programas archivados en los equipos computadorizados y en los medios de almacenamiento electrónico de una forma segura que permita mantener el control de los mismos, y evitar que sean accedidos por personas no autorizadas.

La situación comentada puede propiciar que, al momento de transferir o de descartar los equipos computadorizados y los medios de almacenamiento electrónico, no se considere la eliminación de la información confidencial ni de los programas almacenados en los mismos. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y que la misma sea divulgada o utilizada indebidamente, y ocasionar situaciones que afecten los derechos de terceros por las cuales se responsabilice a la UPR-Cayey.

La situación comentada se atribuye a que el Rector no veló ni le requirió a la Directora Interina de la OSI que desarrollara para su aprobación los procedimientos escritos para el mencionado proceso.

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

La Oficina de OSI tiene que actualizar todos los procedimientos mencionados en el Hallazgo 4 y remitirlos al Rector para su aprobación final. Se estima que el tiempo que pueda tomarle actualizar estos procedimiento podría ser aproximadamente un año, tomando en cuenta que se están adquiriendo nuevos servidores y esto conlleva cambios en los procedimientos y documentación. [Apartado a.]

La Oficina de OSI desarrollará el procedimiento para eliminar la información confidencial y los programas archivados en los equipos computarizados y en los medios de almacenamiento electrónico antes de transferir o descartar los mismos. Se espera que el mismo esté listo para verano del 2011 y aprobado por el Rector.  
[Apartado b.]

### **Hallazgo 5 - Falta de controles físicos y ambientales en los cuartos de distribución de cableado, y deficiencias relacionadas con el diagrama esquemático de la red**

a. La UPR-Cayey tiene 34 cuartos de distribución de cableado ubicados en varios de sus edificios. El examen efectuado el 6 y 8 de julio de 2009 de los controles físicos<sup>6</sup> y ambientales<sup>7</sup> existentes en 20 de estos cuartos, reveló que no existían condiciones de seguridad adecuadas para proteger los equipos de comunicación de la UPR-Cayey, según se indica:

1) Relacionado con los controles físicos:

a) En la OSI no se mantenía un control de acceso adecuado para los cuartos de distribución de cableado<sup>8</sup>. La Directora Interina de la OSI no mantenía bajo su custodia las llaves de 14 cuartos (70 por ciento). Estas eran controladas por el personal de la oficina donde se encontraban localizados dichos cuartos. En 7 de estos cuartos (50 por ciento) las puertas estaban sin seguro, accesibles al personal que laboraba y visitaba dichas oficinas, y en 5 (36 por ciento), los equipos de comunicación estaban instalados en anaqueles abiertos sin ninguna protección. Además, en 9 cuartos (45 por ciento) los gabinetes donde estaban instalados los equipos de comunicación tenían abierto el candado o la cerradura.

---

<sup>6</sup> Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados, por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

<sup>7</sup> Controles diseñados para proteger las instalaciones y los equipos de eventos inesperados que ocurren naturalmente o son ocasionados por el hombre. Entre estos: tormentas, huracanes, ataques terroristas, vandalismo, descargas eléctricas y fallas de equipo.

<sup>8</sup> Una relación de los cuartos de distribución de cableado y de los edificios donde estaban ubicados se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector y al ex-Rector de la UPR-Cayey para comentarios.

- b) En los 20 cuartos de distribución de cableado (100 por ciento) no había un diagrama de los *drops*<sup>9</sup>, y el cableado horizontal de estos no estaba identificado.
- c) En 6 cuartos de distribución de cableado<sup>10</sup> (30 por ciento) los equipos de la red de comunicación no estaban conectados a un generador de energía ininterrumpible (*UPS*, por sus siglas en inglés).
- d) En 4 cuartos de distribución de cableado<sup>10</sup> (20 por ciento) los cables conectados desde los paneles de distribución a los *switches*<sup>11</sup> no estaban organizados.
- e) En 18 cuartos de distribución de cableado<sup>10</sup> (90 por ciento) los cables que van conectados desde los paneles de distribución a los *switches* no estaban identificados.
- f) En 5 cuartos de distribución de cableado<sup>10</sup> (25 por ciento) el cableado del panel del servicio telefónico se encontraba junto a los paneles del cableado de la red.
- g) En cinco cuartos de distribución de cableado<sup>10</sup> los cables de la red no se mantenían dentro de un tubo flexible.
- h) En un cuarto de distribución de cableado<sup>10</sup> (5 por ciento), cerca del gabinete donde se mantenía el equipo de comunicación, pasaba un tubo con cables de corriente eléctrica, lo que puede ocasionar interferencia en la comunicación.

---

<sup>9</sup> Conector de pared para instalaciones de redes.

<sup>10</sup> Véase la nota al calce 8.

<sup>11</sup> Dispositivos de comunicación central que conectan dos o más segmentos de red y permiten que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

## 2) Relacionado con los controles ambientales:

- a) En 13 cuartos de distribución de cableado<sup>12</sup> (65 por ciento) se almacenaban materiales inflamables, tales como: cajas de cartón, detergentes, rollos de papel, *toners* de impresoras, latas de pintura y pintura en aerosol, alfombras plásticas, papel de regalo, adornos de navidad y materiales de oficina.
- b) En 2 cuartos de distribución de cableado<sup>12</sup> (10 por ciento) no se mantenía una temperatura adecuada para la operación de los *switches*. En uno de los cuartos el acondicionador de aire estaba dañado.

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, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso a las áreas donde están ubicados los servidores y los equipos de comunicaciones
- Se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas
- No se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos de comunicación

---

<sup>12</sup> Véase la nota al calce 8.

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada
  - Se utilice equipo y tecnología adecuada para proteger los sistemas.
- b. El examen de la documentación de la configuración o estructura de la red de la UPR-Cayey (diagrama esquemático), suministrada para examen, reveló las siguientes deficiencias:
- 1) El diagrama esquemático constaba de 16 páginas en las cuales se ilustraban los *switches* instalados, el tipo de alambrado utilizado para conectar los componentes de la red, y el nombre del edificio donde estaban ubicados los cuartos de distribución de cableado. En 14 de las 16 páginas del diagrama (88 por ciento) no se incluía la ubicación exacta de los cuartos de distribución de cableado y en 12 (75 por ciento) no se incluía el detalle de las instalaciones realizadas por piso.
  - 2) El diagrama esquemático de la red no indicaba la localización correcta de 12 de los 20 cuartos de distribución de cableado visitados.
  - 3) En el diagrama esquemático no se documentaban las instalaciones, las interconexiones, las descripciones y la configuración de los equipos de telecomunicación conectados a la red, excepto los *switches*, que mantenían en los cuartos de distribución de cableado.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica* de la *Carta Circular Núm. 77-05*, se establece que las agencias deben adquirir e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficiente. 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)a), f) y g)** podrían facilitar que personas no autorizadas tuvieran acceso a los equipos de comunicación, lo que representa un riesgo para la continuidad de los servicios que ofrece la UPR-Cayey, así como la confidencialidad de la información. Además, pudieran ocasionar daños a estos equipos y dificultaría fijar responsabilidades.

Las situaciones comentadas en los **apartados a.1)b), d) y e), y b.** impiden a la UPR-Cayey obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento a la misma. Además, dificultan la atención de problemas de conexión en un tiempo razonable, y planificar eficazmente las mejoras a la red según el crecimiento de sus sistemas.

Las situaciones comentadas en el **apartado a.1)c) y h), y 2)a) y b)** pudieran ocasionar daños y deterioros prematuros a los equipos de la red y a los equipos de computadoras, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos.

Las situaciones comentadas se debían a que la Directora Interina de la OSI no había impartido instrucciones para que:

- Se implantaran medidas de control para la seguridad y el acceso físico de las instalaciones de la red [**Apartado a.**]
- Se actualizara el diagrama esquemático para que el mismo incluya información relevante de su estructura de red. [**Apartado b.**]

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

El Director de OSI impartirá instrucciones para que revisen el acceso físico y seguridad de los gabinetes de comunicaciones. [sic] **[Apartado a.]**

Se actualizará el diagrama esquemático al detalle, el mismo debe estar finalizado para verano del 2011. [sic] **[Apartado b.]**

**Hallazgo 6 - Falta de adiestramientos al personal de la OSI a cargo de la seguridad y de administrar la red**

- a. El personal de la OSI a cargo de la seguridad y de administrar la red, no había recibido adiestramientos continuos sobre la seguridad y la confidencialidad de la información, y las leyes de derechos de autor de los programas computadorizados. Además, no se nos suministró evidencia de que este personal haya recibido adiestramientos periódicos sobre los procedimientos a seguir en caso de emergencia. Estos adiestramientos son necesarios para asegurarse de que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con la seguridad de los sistemas de información.

Una situación similar fue comentada en el *Informe OAIC-2006-03* emitido el 3 de mayo de 2006 por la Oficina de Auditoría Interna de la Junta de Síndicos de la Universidad de Puerto Rico.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, lo siguiente:

- La agencia es responsable de proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y de los beneficios correspondientes.
- El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.

- La agencia es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que les apliquen.

Es norma generalmente aceptada que las dependencias y las entidades gubernamentales identifiquen las necesidades de adiestramiento de cada grupo de usuarios de los sistemas de información, basándose en las áreas en que les falte experiencia y conocimiento. Para identificar las necesidades de los usuarios se debe definir y ejecutar una estrategia para el adiestramiento efectivo y medir los resultados. El establecer un programa de adiestramiento aumenta la efectividad del uso de la tecnología para reducir los errores cometidos por los usuarios, aumenta la productividad y el cumplimiento adecuado de los deberes y las funciones de los empleados.

La situación comentada podría reducir la efectividad de los sistemas computadorizados, y poner en riesgo la seguridad de los empleados y de dichos sistemas. Además, podría impedir la disponibilidad de los sistemas y, por consiguiente, limitar los servicios que presta la UPR-Cayey.

La situación comentada se debía a que la Directora Interina de la OSI no había identificado las necesidades de adiestramiento para su personal a los fines de planificar, coordinar e implantar un plan de adiestramiento continuo para estos.

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

El Director de OSI trabajará un plan de adiestramiento en conjunto con el coordinador de adiestramientos para el personal a cargo de la seguridad y de administrar la red de computadoras y servidores. Por lo costoso de los adiestramientos se espera poder brindarlos para el próximo año fiscal (2011-2012). [sic]

### **Hallazgo 7 - Falta de controles sobre los equipos de la red y deficiencias en su mantenimiento**

a. El examen realizado el 6 y 8 de julio de 2009 sobre el control y la administración de los equipos de la red, en 20 cuartos de distribución de cableado, reveló lo siguiente:

- 1) Veinticinco<sup>13</sup> *switches* y un *UPS* no estaban identificados con número de propiedad.
- 2) Seis<sup>13</sup> *UPS* y dos *switches*, identificados con los números de propiedad no estaban incluidos en el inventario de propiedad de la UPR-Cayey.

Una situación similar a la indicada en el **apartado a.1)** se comentó en el informe de auditoría anterior *CPED-92-10*.

En el *Reglamento para el Control de la Propiedad Mueble de la Universidad de Puerto Rico* del 18 de agosto de 1994, según enmendado, aprobado por la Junta de Síndicos de la UPR se dispone que el Encargado de la Propiedad será responsable de:

- Mantener al día en forma ordenada y actualizada todos los expedientes de propiedad mueble que estén bajo su posesión o la de otros funcionarios o fuera de los límites jurisdiccionales de la unidad de inventario. Esta responsabilidad comienza en el instante en que oficialmente asuma la custodia de la propiedad mueble universitaria.
- Numerar físicamente el activo y registrarlo en los expedientes.
- Hacer pruebas para determinar la confiabilidad del proceso de inventario antes de proceder con la certificación final del inventario.

---

<sup>13</sup> Una relación de los equipos se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector y al ex-Rector de la UPR-Cayey para comentarios.

Las situaciones comentadas le impiden a la UPR-Cayey mantener un control adecuado sobre la propiedad, lo que puede propiciar el uso indebido o la pérdida de la misma, sin que se pueda detectar a tiempo para fijar responsabilidades. Además, dificulta la identificación y la localización de los equipos y le resta confiabilidad a la información existente en el informe de inventario de activos. También dificulta nuestra gestión fiscalizadora.

La situación comentada en el **apartado a.1)** se debe a que la Directora Interina de la OSI no le requirió al personal a cargo de la red de comunicación, que luego de realizada la instalación de dichos equipos por terceros, notificara al personal de la Oficina de Propiedad para que fuera a identificar y numerar dichos equipos para actualizar el inventario.

La situación comentada en el **apartado a.2)** se debe a que el personal que asignó los números de propiedad a los equipos mencionados no actualizó el inventario con dicha información.

- b. Un examen realizado entre mayo y julio de 2009 sobre el mantenimiento a los equipos conectados a la red, reveló que en la OSI no contaban con un itinerario para el mantenimiento preventivo de los mismos, de acuerdo con las recomendaciones del fabricante.

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 los equipos conectados a la red no sean detectadas a tiempo. Esto, a su vez, puede resultar en una falla mayor en la que se interrumpan las operaciones de la UPR-Cayey.

La situación comentada se debía a que la Directora Interina de la OSI no había cumplido con su deber de remitir el borrador del *Plan de Reposición, Actualización y Mantenimiento de Equipos y Software* para la aprobación del Rector. Este incluía como uno de sus objetivos establecer un programa de mantenimiento continuo para los equipos y los programas.

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

En la actualidad todo equipo que se adquiere es instalado por el personal de OSI. El equipo se adquiere mediante orden de compra, propiedad lo recibe, lo identifica, y lo traslada a la oficina solicitante. **[Apartado a.1)]**

La Oficina de Propiedad realiza un inventario anual y actualiza la información en el sistema de Propiedad. **[Apartado a.2)]**

De los equipos que están conectado a la red de comunicación los siguientes están en contrato de mantenimiento: Servidor Alpha, Core Switch principal, y UPS primario para el centro de datos. Los servidores no están en mantenimiento ya que están obsoletos y están próximos a reemplazarse. *[sic]* **[Apartado b.]**

Consideramos las alegaciones del Rector con respecto a los **apartados a.2) y b. del Hallazgo**, pero determinamos que los mismos prevalecen. Esto, debido a que el Rector no nos suministró evidencia de que los equipos mencionados en el **apartado a.2)** fueron incluidos en el inventario anual que realiza la Oficina de Propiedad. Además, con respecto al **apartado b.**, la evidencia suministrada indica que solo tres equipos de los conectados a la red están incluidos en el contrato de mantenimiento.

**ANEJO 1**

UNIVERSIDAD DE PUERTO RICO EN CAYEY  
OFICINA DE SISTEMAS DE INFORMACIÓN  
**MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS  
QUE ACTUARON DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Ygrí Rivera de Martínez	Presidenta	27 jun. 09	17 jul. 09
Ing. Carlos H. del Río Rodríguez	Presidente	23 jul. 08	26 jun. 09
Lcdo. Salvador Antonetti Zequeira	Secretario	23 jul. 08	17 jul. 09

**ANEJO 2**

**UNIVERSIDAD DE PUERTO RICO EN CAYEY  
OFICINA DE SISTEMAS DE INFORMACIÓN  
FUNCIONARIOS PRINCIPALES QUE ACTUARON  
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Ram S. Lamba Bhiranwawali	Rector	23 jul. 08	17 jul. 09
Sra. Rosa Ramírez Rabelo	Directora Interina de la Oficina de Sistemas de Información	16 oct. 08	17 jul. 09
Sr. Edwood Ocasio Vicente <sup>14</sup>	Director de la Oficina de Sistemas de Información	23 jul. 08	31 oct. 08
Sra. María M. Santiago Morales	Decana de Administración Interina	1 jul. 09	17 jul. 09
Sr. Edfel Rivera Rivera	Decano de Administración	23 jul. 08	30 jun. 09
Sra. María Cortés Santos	Directora de Recursos Humanos	23 jul. 08	17 jul. 09
Sra. Miriam González Ortiz	Oficial de la Propiedad	23 jul. 09	17 jul. 09

<sup>14</sup> Del 16 al 31 de octubre de 2008, el señor Ocasio Vicente estuvo disfrutando de una licencia de vacaciones. Por esto, la Sra. Rosa Ramírez Rabelo fue designada Directora Interina de la OSI desde el 16 de octubre de 2008.

