

Principales Papeles
1) agosto / 2012



Secretaría

- 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

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

INFORME DE AUDITORÍA TI-13-01

13 de julio de 2012

Universidad de Puerto Rico en Bayamón

Oficina de Sistemas de Información

(Unidad 5490 - Auditoría 13309)

Período auditado: 19 de junio al 16 de diciembre de 2009

CONTENIDO

	Página
ALCANCE Y METODOLOGÍA	2
CONTENIDO DEL INFORME	2
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	3
COMUNICACIÓN CON LA GERENCIA	5
OPINIÓN Y HALLAZGOS	5
1 - Falta de un informe de avalúo de riesgos sobre los sistemas de información computadorizados	6
2 - Falta de controles físicos y ambientales en la OSI	7
3 - Deficiencias relacionadas con los controles ambientales y físicos en las áreas de distribución de cableado, y falta de diagramas esquemáticos de la red	13
4 - Deficiencias relacionadas con los parámetros de seguridad del servidor primario	17
5 - Falta de documentación sobre las revisiones de los registros de seguridad del Sistema de Información Estudiantil y de un registro sobre el uso de conexiones remotas	19
6 - Falta de aprobación del plan de contingencias y de las políticas, las normas y los manuales relacionados con las operaciones de la OSI	21
7 - Falta de documentación de los cambios realizados al SIE	23
8 - Lista de servidores de la OSI no actualizada, y falta de diagramas de las redes departamentales y de registros de los servidores conectados a estas	24
RECOMENDACIONES	27
AGRADECIMIENTO	29
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS DURANTE EL PERÍODO AUDITADO	30
ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	31

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

13 de julio de 2012

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 Bayamón (UPRB) para determinar si las mismas se efectuaron 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. Hicimos 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.

**ALCANCE Y
METODOLOGÍA**

La auditoría cubrió del 19 de junio al 16 de diciembre 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, tales como: entrevistas, inspecciones físicas, examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas, pruebas y análisis de procedimientos de control interno y de otros procesos, y confirmaciones de información pertinente.

**CONTENIDO DEL
INFORME**

Este *Informe* contiene ocho hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, los controles de la red de comunicaciones, el control de acceso lógico y físico, la evaluación de la continuidad del

servicio, y el desarrollo y el control de los cambios de las aplicaciones. El mismo está disponible en nuestra página en Internet: <http://www.ocpr.gov.pr>.

**INFORMACIÓN SOBRE
LA UNIDAD AUDITADA**

La UPRB fue creada por el Consejo de Educación Superior mediante la *Certificación Núm. 16 del 14 de julio de 1970*. Esto, con el propósito de ofrecer programas de grados asociados y bachilleratos en áreas de interés para la comunidad, con un personal docente que tenga conocimientos y destrezas de los últimos avances tecnológicos.

Mediante la *Ley 16-1993*, se enmendó el Artículo 3 de la *Ley Núm. 1 del 20 de enero de 1966, Ley de la Universidad de Puerto Rico*. Esto, para eliminar el Consejo de Educación Superior como cuerpo rector de la UPR y crear la Junta de Síndicos (Junta). Mediante la *Ley 65-2010*, se enmendó este Artículo, a los fines de ampliar la composición de los miembros de la Junta. A partir de esta fecha, la misma está compuesta por 17 miembros, de los cuales 10 son profesionales destacados en distintos sectores, 4 son egresados de la Universidad de Puerto Rico, 2 son profesores y 1 es estudiante. Los profesores y el estudiante son elegidos por representantes del personal docente y del estudiantado en la Junta Universitaria, respectivamente.

Efectivo el 1 de julio de 1998, la Junta de Síndicos le otorgó la autonomía a la UPRB, mediante la *Certificación Núm. 151 del 24 de junio de 1998*. Durante el período de transición hacia la autonomía otorgada, del 1 de julio al 30 de septiembre de 1998, se transfirieron a la UPRB todas las funciones operacionales, administrativas y docentes, incluidas la administración del presupuesto.

La administración y la supervisión de las operaciones de la UPRB 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. El Rector preside la Junta Administrativa y el Senado Académico. Al Rector, le responden los decanatos de Asuntos

Académicos, de Asuntos Administrativos, y de Asuntos Estudiantiles; las oficinas de Sistemas de Información, de Presupuesto, y de Asuntos Legales; y el Procurador Estudiantil.

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

La OSI de la UPRB estaba compuesta por la División de Desarrollo de Tecnologías de Información, la División de Administración de Redes y Servicio al Usuario y la División de Operaciones. Además, contaba con 1 Directora, 1 Subdirectora, 1 Secretaria Administrativa V, 1 Director de Desarrollo de Tecnologías de Información, 1 Especialista en Tecnologías de Comunicación I, 1 Coordinador de Servicios al Usuario I, 1 Coordinador de Servicios al Usuario II, 1 Supervisora de Operaciones de Computador Electrónico, 2 especialistas de tecnologías de información, 2 especialistas de equipo de computación y telecomunicaciones, 2 técnicos de tecnología de información, 1 Operador de Computador Electrónico I y 1 Operador de Computador Electrónico II. A la fecha de nuestra auditoría, la UPRB contaba con 44 servidores para realizar sus operaciones.

Los recursos para financiar las actividades operacionales de la UPRB provienen principalmente de fondos federales, ingresos propios, préstamos y bonos para efectuar mejoras permanentes, y de asignaciones especiales canalizados por la Administración Central de la UPR. El presupuesto de la UPRB para los años fiscales del 2007-08 al 2009-10 ascendió a \$42,485,116, \$43,178,271 y \$41,526,482, respectivamente.

Los recursos asignados por la UPRB para las operaciones de la OSI durante los años fiscales del 2007-08 al 2009-10 ascendieron a \$837,798, \$822,135 y \$883,396, respectivamente.

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

**COMUNICACIÓN CON
LA GERENCIA**

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Dr. Arturo Avilés González, entonces Rector Interino de la UPRB, mediante carta de nuestros auditores del 28 de enero de 2010. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

El 8 de febrero de 2010, el doctor Avilés González remitió sus comentarios sobre los hallazgos incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al doctor Avilés González, Rector de la UPRB, y a la Prof. Irma R. Schmidt Soltero, ex-Rectora de la UPRB, para comentarios, por cartas del 17 de noviembre de 2011.

El 1 de diciembre de 2011, la Sra. María D. Ruiz Cintrón, Ayudante Ejecutiva de la Oficina de Rectoría, en representación del Rector, solicitó una prórroga para contestar el borrador de los **hallazgos** de este *Informe*. El 2 de diciembre de 2011, le concedimos una prórroga hasta el 6 de diciembre de 2011, para remitir sus comentarios. El Rector contestó el borrador de los **hallazgos** de este *Informe*, mediante carta recibida en esta Oficina el 6 de diciembre de 2011. Además, la ex-Rectora remitió sus comentarios sobre el **Hallazgo 8** de este *Informe* mediante carta del 9 de diciembre de 2011. Los comentarios de estos funcionarios fueron considerados en la redacción final de este *Informe*, y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OSI de la UPRB, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, los controles de la red de comunicaciones, el control de acceso lógico y físico, la evaluación de la continuidad de servicio, y el desarrollo y el control de los cambios de las

aplicaciones, se realizaron sustancialmente de acuerdo con la ley y la reglamentación aplicables; excepto por los **hallazgos del 1 al 8** que se comentan a continuación.

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

Situación

a. Un avalúo de riesgos de los sistemas de información es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. 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 14 de septiembre de 2009, en la UPRB no se había realizado un avalúo de riesgos sobre los sistemas de información computadorizados.

Criterio

Esta situación es contraria a lo establecido 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.

Efecto

La situación comentada impide a la UPRB estimar 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 la pérdida de información.

Causa

La situación comentada se atribuye a que los rectores de la UPRB no habían promulgado una directriz sobre la preparación del avalúo de riesgos de los sistemas de información, como se establece en la *Carta Circular Núm. 77-05*.

Comentarios de la Gerencia

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

Se realizará el mismo por la Directora de la Oficina de Sistemas de Información y la Coordinadora de Auditorías durante el mes de enero de 2012. [sic]

Véanse las recomendaciones de la 1 a la 3.

Hallazgo 2 - Falta de controles físicos y ambientales en la OSI

Situaciones

- a. La OSI contaba con un área de recepción, un área de oficinas y un Cuarto de Máquinas donde estaban ubicados los servidores y los equipos de comunicaciones de las redes principales de la UPRB. La Directora de la OSI era la encargada de establecer los controles de acceso físicos¹ y ambientales² de la OSI, y de coordinar con el Decano de Asuntos Administrativos las mejoras físicas necesarias para este propósito. Además, el Decano de Asuntos Administrativos

¹ 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.

² Controles diseñados para proteger las instalaciones y los equipos de eventos inesperados que ocurren naturalmente o son ocasionados por el hombre. Entre estos, tormentas, erupciones volcánicas, huracanes, tornados, ataques terroristas, vandalismo, descargas eléctricas y fallas de equipo.

era responsable de autorizar al Oficial de Propiedad a reproducir y distribuir las llaves que permitían acceso a la OSI. Para mantener un sistema de registro de las llaves, el Oficial de Propiedad mantenía un expediente para cada custodio de llave en el que debía incluir los formularios *Solicitud de Llaves*, *Recibo de Llaves* y *Devolución de Llaves*, según fuera necesario. Esto, para documentar la expedición, el cambio y la devolución de llaves, candados y cerraduras.

El examen efectuado entre el 17 de noviembre y el 3 de diciembre de 2009 de los controles ambientales y físicos, reveló que no se habían establecido las condiciones de seguridad física³ adecuadas para proteger los sistemas de información computadorizados de la OSI, según se indica:

- 1) Relacionado con los controles ambientales:
 - a) Los paneles acústicos del techo del Cuarto de Máquinas tenían manchas de humedad que evidenciaban la existencia de filtraciones de agua en el área. Además, observamos que los equipos de comunicaciones estaban cubiertos con un material plástico para protegerlos de posibles daños por filtraciones de agua. Los empleados de la OSI habían instalado el plástico desde agosto de 2009 para proteger los equipos de las posibles filtraciones durante la época de huracanes, y no lo retiraban durante horas laborables. Esta práctica no es recomendada debido a que limita la ventilación del aire, lo que podría calentar y dañar los equipos, y aumenta la posibilidad de un incendio.
 - b) La planta generadora de electricidad alterna de la UPRB no respondió al encendido automático durante una interrupción del servicio eléctrico ocurrida el 17 de noviembre de 2009. Además, las baterías de los servidores no tenían la

³ Incluye los controles y los procedimientos establecidos para proteger a las personas, la información, los equipos, los sistemas y las instalaciones al utilizar mecanismos de seguridad que incluyen el diseño y la ubicación de las instalaciones, los componentes ambientales, las medidas de respuesta de emergencia, el control de acceso, la detección de intrusos y la protección contra fuego y pérdida de energía.

capacidad suficiente para producir los respaldos de información y apagar los sistemas de forma ordenada y segura.

- 2) Relacionado con los controles físicos, las llaves que permitían acceso a la OSI no se controlaban adecuadamente, según se indica:
 - a) Al 3 de diciembre de 2009, los decanos interinos de Asuntos Académicos, de Asuntos Administrativos y Auxiliar de Asuntos Administrativos; el Especialista de Salud y Seguridad; el Director de Planta Física; y el Supervisor de Construcción, podían acceder a la OSI mediante la llave conocida como *Grand Master* que le había asignado el Oficial de Propiedad. Estos funcionarios no desempeñaban tareas relacionadas con la OSI. Además, los decanos interinos de Asuntos Académicos, y Auxiliar de Asuntos Administrativos; y el Supervisor de Construcción no estaban incluidos entre el personal autorizado para ser custodio de esta llave.
 - b) En 19 formularios *Solicitud de Llaves*⁴, que fueron preparados entre el 18 de julio de 2006 y el 5 de octubre de 2009, no se incluyó la firma del Decano de Asuntos Administrativos para autorizar los mismos. En su lugar, estos formularios fueron autorizados por la Rectora de la UPRB. No encontramos, además, que se notificara sobre estas autorizaciones al Decano de Asuntos Administrativos, correspondiente.

⁴ Una relación de estos formularios se incluyó en el borrador de los **hallazgos** del *Informe* remitido al Rector y a la ex-Rectora de la UPRB para comentarios.

- c) Un Operador de Computador Electrónico I y un Oficial de Propiedad no habían completado el formulario *Recibo de Llaves*. En este formulario el usuario reconocía sus responsabilidades y deberes en cuanto a la custodia y al uso de las llaves asignadas.
- d) En la Oficina de Propiedad no se mantenía un registro de llaves que incluyera de forma accesible y organizada la información sobre las copias de las llaves de la OSI y demás instalaciones, y el personal custodio de estas. Para obtener dicha información, el Oficial de Propiedad tenía que ir a los expedientes de cada empleado, los cuales se mantenían en la Oficina de Propiedad.

Criterios

Las situaciones comentadas en el **apartado a.1)a)** son contrarias a lo establecido en la Sección *Protección de los Recursos Informáticos* de los *Estándares para la Utilización Aceptable de Recursos de Tecnología Informática (Estándares)*, aprobados el 7 de abril de 2008 por la Vicepresidenta de Investigación y Tecnología de la UPR.

La situación comentada en el **apartado a.1)b)** es contraria a lo establecido en la Sección *Disposiciones* de la *Política Institucional para la Interconexión y Seguridad de la Infraestructura de Comunicaciones de la UPRB (Política Institucional de la UPRB)*, aprobada el 9 de julio de 2007 por la Rectora de la UPRB.

Las situaciones comentadas en el **apartado a.2)a) y d)** son contrarias a lo establecido en las secciones A y B del Artículo I, *Organización del Sistema de Control de Llaves*, de las *Normas y Procedimientos para la Otorgación y Control de Llaves Oficiales en la Universidad de Puerto Rico en Bayamón (Normas y Procedimientos)*, aprobadas el 28 de octubre de 2002 por el Rector de la UPRB.

Las situaciones comentadas en el **apartado a.2)b) y c)** son contrarias a lo establecido en la Sección A del Artículo II, *Disposiciones Normativas*, y en la Sección A del Artículo III, *Procedimientos*, respectivamente, de las *Normas y Procedimientos*.

Efectos

La situación comentada en el **apartado a.1)a)** puede propiciar daños a las instalaciones y a los equipos, pérdida de información sensitiva, así como provocar eventos de interrupción de servicios que afectarían la continuidad de las operaciones de los sistemas de información computadorizados de la UPRB. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

La situación comentada en el **apartado a.1)b)** ocasionó una interrupción el 17 de noviembre de 2009, por aproximadamente 1 hora y 20 minutos, de los servicios ofrecidos por la UPRB, y la activación de la alarma de temperatura en el Cuarto de Máquinas. Además, provocó que se corrompiera la base de datos de los usuarios de la red inalámbrica.

Las situaciones comentadas en el **apartado a.2)a)** pueden propiciar que personas no autorizadas y ajenas a la OSI, por error o intencionalmente, causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y la divulgación indebida de información, dificulta la adjudicación de responsabilidades a las personas que cometan estos actos, y podría afectar adversamente el funcionamiento de la red y la continuidad de las operaciones. Además, las situaciones comentadas en el **apartado a.2) del b) al d)** no le permitían al Oficial de Propiedad mantener un control adecuado de las llaves asignadas a los funcionarios y a los empleados de la UPRB. Esto podría ocasionar el acceso no autorizado a las áreas restringidas, lo que resultaría en otras consecuencias adversas.

Causas

Las situaciones comentadas en el **apartado a.1)** se debían, en parte, a que la Directora de la OSI:

- No había coordinado con el Decano de Asuntos Administrativos para que este tomara las medidas necesarias para corregir las deficiencias comentadas.
- No había efectuado gestiones para que se adquirieran baterías para los servidores, que en caso de fallas en la planta generadora le pudieran proveer a estos la capacidad necesaria para efectuar los respaldos y bajar los sistemas de forma ordenada. **[Apartado a.1)b)]**

Las situaciones comentadas en el **apartado a.2)** se debían, en parte, a que:

- Las *Normas y Procedimientos* no requerían que las cerraduras de la OSI utilizaran llaves distintas a las de las demás instalaciones de la UPRB. **[Apartado a.2)a)]** Además, no le requerían al Oficial de Propiedad mantener un registro por área que le facilitara obtener la información de todo el personal que tenía llave de acceso a cada una de estas. **[Apartado a.2)d)]**
- El Oficial de Propiedad no mantenía registros completos y actualizados sobre las autorizaciones y los recibos relacionados con la asignación de llaves al personal de la UPRB. **[Apartado a.2)b) y c)]**

Comentarios de la Gerencia

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

[...] Se solicitó a Planta Física que el Técnico de Refrigeración corrija el problema a la brevedad posible. *[sic]* **[Apartado a.1)a)]**

[...] A partir del 9 de julio de 2011, la compañía [...] a través de un contrato de servicios personales no misceláneos realizó las labores de mantenimiento a la planta generadora y al sistema eléctrico [...] de toda la Institución. *[sic]* **[Apartado a.1)b)]**

[...] El procedimiento de uso y control de llaves que dan acceso a la Oficina de Sistemas de Información se encuentra en revisión por parte del Decanato de Asuntos Administrativos. [sic] [Apartado a.2)]

Véanse las recomendaciones 1, 2, 4.a.1) y b., y 5.

Hallazgo 3 - Deficiencias relacionadas con los controles ambientales y físicos en las áreas de distribución de cableado, y falta de diagramas esquemáticos de la red

Situaciones

a. La red de comunicaciones principal de la OSI contaba con 20 áreas de distribución de cableado ubicados en 18 edificios de la UPRB. En estas áreas se habían instalado gabinetes y estantes para proteger los equipos de comunicaciones que mantenían las conexiones necesarias para interconectar las computadoras que recibían servicio de la red. El examen efectuado entre el 17 de noviembre y el 8 diciembre de 2009 sobre los controles ambientales y físicos en las áreas de distribución del cableado donde estaban instalados los equipos de comunicaciones de la UPRB, reveló que no existían las condiciones de seguridad física adecuadas para proteger los equipos de comunicación, según se indica:

1) Relacionado con los controles ambientales:

- a) En un área⁵, el estante donde se encontraban los equipos de comunicaciones estaba cubierto con un toldo plástico para proteger los mismos de daño por filtraciones de agua. Esta práctica no es recomendada porque limita la ventilación del aire, lo que podría calentar y dañar los equipos, y aumenta la posibilidad de un incendio. Además, no garantiza la protección de los equipos contra las filtraciones.
- b) En un área⁵ donde se encontraba ubicado el gabinete, no se había instalado un acondicionador de aire para controlar las altas temperaturas.

⁵ La ubicación de las áreas de distribución de cableado se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector y a la ex-Rectora de la UPRB para comentarios.

- c) En ocho áreas⁶, no había extintores. Además, en dos áreas⁶ los extintores instalados cerca de los gabinetes no habían sido revisados desde julio de 2008.
 - d) En siete áreas⁶, los equipos de comunicación ubicados en los gabinetes estaban cubiertos por partículas de polvo, lo que denotaba falta de mantenimiento.
 - e) En un área⁶, los cables que se conectaban a los equipos de comunicaciones que se encontraban en el gabinete se mantenían junto a los cables eléctricos. Esta práctica no es recomendada debido a que las interferencias electromagnéticas podrían dañar la señal y, en caso de fuga la electricidad podría transmitirse hasta los dispositivos y quemarlos.
- 2) Relacionado con los controles físicos:
- a) En 11 áreas⁶ los cables que se conectaban a los equipos de comunicaciones ubicados en los gabinetes, no se mantenían organizados y no habían sido identificados. Además, en dos áreas⁶ los cables que se conectaban a los equipos de comunicaciones no estaban organizados. Esto es necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones.
 - b) En nueve áreas⁶ los cables de entrada y salida conectados a los equipos de comunicación que se encontraban en los gabinetes estaban expuestos desde el gabinete hasta el techo. Además, la misma situación se repetía en un área, pero ocurría por el suelo de las instalaciones.
 - c) En un área⁶ el gabinete estaba ubicado dentro del baño de damas.

⁶ Véase la nota al calce 5.

- b. En 16 áreas⁷ no se mantenían en los gabinetes diagramas esquemáticos que ilustraran las conexiones establecidas con los equipos.

Criterios

Las situaciones comentadas en el **apartado a.1) y 2)b) y c)** son contrarias a lo establecido en la Sección *Disposiciones* de la *Política Institucional de la UPRB*.

Las situaciones comentadas en el **apartado a.2)a) y b)** son contrarias a lo establecido en la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológicas*, de la *Carta Circular Núm. 77-05*.

Las mejores prácticas en el campo de la tecnología de información sugieren que para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados es necesario que se identifique adecuadamente el cableado de conexión a la red, de forma que, se puedan corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada. **[Apartados a.2)a) y b.]**

Efectos

Las situaciones comentadas en el **apartado a.1) del a) al d)** pueden propiciar daños a los equipos, así como provocar eventos de interrupción de servicios que afectarían la continuidad de las operaciones de los sistemas de información computadorizados de la UPRB. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

Las situaciones comentadas en los **apartados a.2)a) y b.** impiden a la UPRB identificar los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificultan atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

⁷ Véase la nota al calce 5.

Las situaciones comentadas en el **apartado a.1)e), y 2)b) y c)** pueden propiciar que personas ajenas a las operaciones de la red tengan acceso a los cables y a los equipos, lo que representa un riesgo para la continuidad de los servicios que ofrece la UPRB, así como para la confidencialidad de la información. Además, pudieran ocasionar daños a los equipos de comunicación y dificultarían fijar responsabilidades. Por otro lado, la situación comentada en el **apartado a.1)e)** podría causar interferencia en las comunicaciones.

Causas

Las situaciones comentadas en los **apartados a.1)d), 2)a) y c), y b.** obedecen a que la Directora de la OSI no había establecido controles de seguridad físicos y ambientales adecuados para proteger los equipos de comunicaciones ubicados en los gabinetes, y sus respectivas conexiones. Además, no había coordinado con el Decano de Asuntos Administrativos para que este tomara las medidas necesarias para corregir las deficiencias comentadas en el **apartado a.1) del a) al c) y e), y 2)b).**

Comentarios de la Gerencia

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

Durante el periodo de huracanes (junio a noviembre) se coloca un plástico a la parte superior de los gabinetes por si existe un evento fuerte de lluvia que provoque filtraciones [...] Se establece un calendario de trabajo para removerlos cuando culmina la temporada de huracanes. **[Apartado a.1)a]**

Se realizó una limpieza de todos los gabinetes y se instruyó a [...] para que mantenga un calendario de trabajo para realizar una limpieza periódica en los gabinetes de comunicaciones. **[Apartado a.1)d]**

Se organizó e identificó el cableado en la mayoría de los gabinetes; queda pendiente atender los gabinetes en el CRA. **[Apartado a.2)a]**

Además, el Rector informó que las situaciones comentadas en los **apartados a.2)b) y b.** se encuentran en proceso de ser atendidas.

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, mantener por seis meses los equipos encendidos dentro de un estante cubierto con plástico. De ser necesario, los plásticos deben utilizarse durante el período en que ocurre el huracán, con los equipos apagados.

Véanse las recomendaciones 1, 2 y, 4.a.2) y c.

Hallazgo 4 - Deficiencias relacionadas con los parámetros de seguridad del servidor primario

Situaciones

- a. El examen efectuado el 12 de agosto de 2009 sobre los parámetros de control de acceso y de seguridad definidos en el sistema operativo del servidor primario, reveló las siguientes deficiencias en la utilización de las opciones que permiten controlar la seguridad de las cuentas de los usuarios:
 - 1) Existían deficiencias en la activación de las políticas relacionadas con las cuentas de acceso (*Account Policies*), según se indica:
 - a) No se requería un mínimo de días para que el sistema le permitiera al usuario cambiar la contraseña nuevamente (*Minimum Password Age*). El día del cambio de la contraseña, los usuarios podían cambiarla dos veces y reutilizar la contraseña anterior.
 - b) No se había definido un término fijo de intentos de acceso sin éxito a los recursos de la red para que el sistema deshabilitara automáticamente las cuentas de acceso (*No account lockout*).

- 2) No se había activado la política de auditoría (*Audit Policy*) para que el sistema produjera, un registro, de ocurrir los siguientes eventos:
 - a) El encendido y apagado de la computadora (*Restart and Shutdown*)
 - b) Los accesos a los archivos, cartapacios (*folders*) e impresoras (*File/Object Access*)
 - c) Las acciones ejecutadas de los procesos (*Process Tracking*)
 - d) Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Security Policy Changes*)
 - e) El uso de los privilegios del usuario (*Use of User Right*)
 - f) El acceso al directorio de servicio (*Directory Service Access*).

Crterios

Estas situaciones son contrarias a lo establecido en la Parte VII, *Derechos y Responsabilidades de la Universidad*, de la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico (Política Institucional de la UPR)*, aprobada mediante la *Certificación Núm. 35* del 19 de febrero de 2008 por la Junta de Síndicos.

Además, la situación comentada en el **apartado a.2)** es contraria a lo establecido en la Sección *Definición de una Respuesta Apropiaada a un Incidente Crítico* de la *Política y Procedimiento para Documentar, Manejar y Resolver Incidentes Técnicos (Política de Incidentes Técnicos)*, aprobada el 10 de julio de 2007 por la Rectora.

Efectos

La situación comentada en el **apartado a.1)** propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta.

La situación comentada en el **apartado a.2)** impide a la UPRB mantener un registro de los eventos inusuales o los problemas ocurridos en la red que le permitiera al Especialista en Tecnologías de Comunicación I tomar a tiempo las medidas correctivas o preventivas necesarias.

Causa

Las situaciones comentadas se debían a que la Directora de la OSI no se aseguró de que el Especialista en Tecnologías de Comunicación I, quien era el encargado de administrar la red de comunicaciones de la UPRB, pusiera en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo del servidor.

Comentarios de la Gerencia

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

Se activaron las políticas de *Minimum Password Age* y *Account Lockout*. [**Apartado a.1)**]

Se activó el *Audit Policy* para que se registren los eventos indicados en el hallazgo. [**Apartado a.2)**]

Véanse las recomendaciones 1, 2 y 4.d.

Hallazgo 5 - Falta de documentación sobre las revisiones de los registros de seguridad del Sistema de Información Estudiantil y de un registro sobre el uso de conexiones remotas

a. La UPRB contaba con el Sistema de Información Estudiantil (SIE) mediante el cual se procesaba la información sobre los estudiantes y los ofrecimientos académicos. A la fecha de nuestra auditoría, el SIE producía los siguientes registros de eventos de seguridad:

- *Accounting* - Proveía información sobre los usuarios que utilizaron el sistema, la fecha y qué archivos fueron utilizados.
- *Shoaudit* - Proveía información sobre los eventos de seguridad.
- *Loginfailure* - Proveía información sobre los intentos fallidos de un usuario en el sistema.

El 17 de septiembre de 2009, la Directora de la OSI nos informó que no se mantenía la documentación de todas las revisiones periódicas

que la Subdirectora de la OSI y el Especialista en Tecnologías de Comunicación I efectuaban a estos registros de eventos de seguridad. Solo se documentaban las revisiones producto de una investigación motivada por una querrela o solicitud formal.

- b. El 10 de diciembre de 2009, la Directora de la OSI nos certificó que no mantenía un registro relacionado con el uso de conexiones remotas para acceder los sistemas de información de la UPRB.

Criterios

Las situaciones comentadas se apartan de lo establecido en la Parte VII de la *Política Institucional de la UPR*, y en las secciones *Definición de una Respuesta Apropriada a un Incidente Crítico* y *Procedimiento de Administración y Utilización de los Recursos* de la *Política de Incidentes Técnicos*.

Efectos

La situación comentada en el **apartado a.** priva a la UPRB de la información sobre la evaluación de incidentes de seguridad ocurridos, la cual es necesaria para identificar los riesgos del SIE y establecer medidas adicionales de seguridad.

La situación comentada en el **apartado b.** priva a la UPRB de la información necesaria para revisar el uso de las conexiones de acceso remoto a los sistemas, lo que propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser identificados, detectados y corregidos a tiempo, y poder fijar responsabilidades, en caso de ser necesario.

Causas

La situación comentada en el **apartado a.** se debía, en parte, a que la OSI no contaba con un Especialista de Sistemas Operativos. Además, la Directora de la OSI no había impartido instrucciones para que el personal asignado a revisar los registros del SIE mantuviera documentación de todas las revisiones efectuadas.

La situación comentada en el **apartado b.** se debió a que la Directora de la OSI no había impartido instrucciones para que se configurara un registro de los accesos, mediante conexiones remotas, a los sistemas de información de la UPRB.

Comentarios de la Gerencia

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

La OSI no cuenta con un Especialista en Sistema Operativo que es la persona que debe realizar monitoreo periódico del sistema y revisar estos informes. [sic] [**Apartado a.**]

Véanse las recomendaciones 1, 2 y 4.e.

Hallazgo 6 - Falta de aprobación del plan de contingencias y de las políticas, las normas y los manuales relacionados con las operaciones de la OSI

Situación

a. En nuestro examen sobre las versiones revisadas del plan de contingencias y de las políticas, las normas y los manuales relacionados con las operaciones de la OSI, determinamos que los siguientes no habían sido aprobados:

- *Plan de Contingencias OSI-UPRB*, revisado en mayo de 2009
- *Política Institucional de la UPRB*, revisada en mayo de 2009
- *Políticas de Uso y Seguridad de la Red Inalámbrica*, revisadas en mayo de 2009
- *Política y Procedimientos para Documentar, Manejar y Resolver Incidentes Técnicos*, revisada en mayo de 2009
- *Política de Publicación de Páginas en el Web*, revisada en mayo de 2009
- *Normas de Seguridad OSI – UPRB*, revisadas en mayo de 2009
- *Normas de Documentación y Mantenimiento de Programas*, revisadas en mayo de 2009

- *Normas y Medidas de Seguridad Dirigidas al Usuario de Tecnología de Información*, revisadas en mayo de 2009
- *Manual de Operadores*, revisado el 20 de febrero de 2009⁸
- *Manual de Referencia Networking*, revisado el 3 de junio de 2009
- *Manual de Resguardos de Datos*, revisado el 20 de febrero de 2009
- *Manual de Procedimientos para la creación y eliminación de cuentas a usuarios de los sistemas Alpha-DS20e Open VMS 7.2-2, Dell PowerEdge 2500 Windows 2003 Google Applications for Education (GAE)*, revisado en abril de 2009.

Una situación similar se comentó en el informe de auditoría anterior CPED-93-5.

Criterio

Esta situación es contraria a lo establecido en el Artículo 18, Sección 18.2 del *Reglamento General de la Universidad de Puerto Rico*, según enmendado, aprobado 16 de febrero de 2002 por la Junta de Síndicos.

Efecto

La situación comentada podría 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.

Causa

La situación comentada se debía a que la ex-Rectora había remitido las políticas, las normas y los procedimientos para la evaluación de la Oficina de Auditoría Interna de la UPR, y debido al retraso en este proceso permitió que se circularan los mismos antes de su aprobación final.

⁸ La versión anterior al *Manual de Operadores* se llamaba *Manual de Procedimientos de Operaciones*.

Comentarios de la Gerencia

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

Se impartió instrucciones para su revisión y posterior trámite a la Junta Administrativa para su aprobación. [sic]

Véanse las recomendaciones 1, 2 y 6.

Hallazgo 7 - Falta de documentación de los cambios realizados al SIE

Situaciones

- a. La OSI contaba con un Director de Desarrollo de Tecnologías de Información responsable de autorizar los cambios efectuados a la programación del SIE. Entre el 1 de junio de 2008 y el 31 de julio de 2009, el personal de programación de la OSI había efectuado 35 cambios al SIE. En nuestro examen sobre la documentación de cinco de estos cambios, determinamos las siguientes deficiencias:
 - 1) Los formularios *Solicitud de Creación o Cambios en Programación* no fueron preparados para documentar la solicitud y autorización para efectuar los cinco cambios examinados. Dichos cambios se solicitaron mediante correo electrónico.
 - 2) La documentación de los cinco cambios examinados no incluía evidencia de las pruebas realizadas por el personal de programación para determinar la efectividad de los mismos ni de sus resultados. Además, no incluía el formulario *Aceptación del Usuario* mediante el cual se documentaba la satisfacción del usuario con los cambios efectuados.
 - 3) Para cuatro cambios, los formularios *Solicitud para Pase de Programado a Ambiente de Producción* no fueron preparados para documentar la autorización requerida para actualizar las versiones de los programas que se mantenían en producción.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la Sección *Procedimiento para Creación o Cambios a Programas en Producción* de las *Normas de Documentación y Mantenimiento de Programas*, aprobadas el 11 de julio de 2007 por la Rectora.

Efecto

Las situaciones comentadas impiden mantener un control adecuado de los cambios efectuados al SIE y podrían afectar la confiabilidad de la información procesada en este. También pueden dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas.

Causa

Las situaciones comentadas se atribuyen a que la Directora de la OSI no se aseguró de que el Director de Desarrollo de Tecnologías de Información documentara adecuadamente los procesos relacionados con el desarrollo y el cambio de aplicaciones.

Véanse las recomendaciones 1, 2 y 4.f.

Hallazgo 8 - Lista de servidores de la OSI no actualizada, y falta de diagramas de las redes departamentales y de registros de los servidores conectados a estas**Situaciones**

- a. La UPRB contaba con un Especialista en Tecnologías de Comunicación I. Este era responsable por el funcionamiento de los 25 servidores que se mantenían en el Cuarto de Máquinas de la OSI y que estaban conectados a la red de la UPRB. Esta contaba, además, con 19 servidores adicionales que se mantenían conectados a las redes departamentales incluidas en el dominio de la UPRB, y que eran administrados por personal técnico que no respondía a la OSI, según se indica:
 - Un Especialista en Comunicaciones administraba los tres servidores del Cuarto de Máquinas del Centro de Recursos para el Aprendizaje.

- Un Especialista en Equipo Computacional administraba los 12 servidores del Centro de Cómputos del Departamento de Ciencias y Tecnología.
- Un Especialista en Equipo de Computación y Telecomunicaciones administraba los tres servidores del Centro de Cómputos del Departamento de Ingeniería.
- Un Mecánico Eléctrico administraba el servidor ubicado en el Centro de Cómputos del Departamento de Electrónica.

El examen realizado sobre el registro de los servidores de la UPRB y los diagramas de la red reveló las siguientes deficiencias:

- 1) Al 14 de septiembre de 2009, la lista de servidores mantenida por el Especialista en Tecnologías de Comunicación I, no incluía seis servidores⁹ que habían sido instalados en el Cuarto de Máquinas. El 27 de enero de 2010, la Directora de la OSI certificó que estos servidores fueron instalados entre el 23 de octubre de 2006 y el 3 de febrero de 2009.
- 2) Al 2 de diciembre de 2009, el Especialista en Comunicaciones, el Especialista en Equipo Computacional, el Especialista en Equipo de Computación y Telecomunicaciones, y el Mecánico Eléctrico, quienes fungían como administradores de las redes departamentales, no mantenían los diagramas esquemáticos que permitieran identificar las conexiones y el cableado de las redes. Además, no mantenían los registros de los servidores conectados a estas redes.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la en la Parte VII de la *Política Institucional de la UPR*.

⁹ Los números de propiedad de estos servidores se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector y a la ex-Rectora de la UPRB para comentarios.

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 los equipos principales y de las conexiones, que permitan corregir a tiempo problemas de comunicación de la red, detectar cualquier conexión no autorizada y planificar adecuadamente los cambios programáticos y de infraestructura.

Efectos

Las situaciones comentadas impiden a la UPRB tener un conocimiento completo de los componentes de sus redes, y dificultan mantener control eficaz en la administración y el mantenimiento de las mismas. Además, dificultan la planificación efectiva de las mejoras a estas redes, según el crecimiento de sus sistemas.

Causa

Las situaciones comentadas se atribuyen a que la Rectora no había establecido procedimientos para requerir al Especialista en Tecnologías de Comunicación I y a los administradores de las redes departamentales que mantengan un registro actualizado de los servidores, los componentes de las redes a su cargo y su interconexión, y que remitan los mismos a la Directora de la OSI.

Comentarios de la Gerencia

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

Los servidores que tienen otros departamentos académicos [...] son servidores que están incluidos en el dominio [...] que administra la OSI; aunque los servidores los administra el personal técnico adscrito a los departamentos. [Apartado a.2)]

En la carta de la ex-Rectora, esta nos indicó lo siguiente:

El trabajo de la OSI es uno altamente técnico, complejo y especializado que sólo entiende con claridad el personal cualificado. La Rectoría no puede estar al tanto de esos detalles si alguien de esa oficina (presumiblemente el director o directora) no lo trae a su atención. Entiendo que al comenzar es esa posición la [...] estaba poniendo en orden múltiples asuntos que dejó en atraso el anterior director. [sic]

Consideramos las alegaciones de la ex-Rectora con respecto a este **Hallazgo**, pero determinamos que el mismo prevalece porque la aprobación de reglamentación necesaria para controlar las operaciones internas de la UPRB corresponde al Rector.

Véanse las recomendaciones 1, 2 y 7.

RECOMENDACIONES**A la Junta de Síndicos de la Universidad de Puerto Rico**

1. Ver que el Presidente de la Universidad cumpla con la **Recomendación 2** de este *Informe*. [Hallazgos del 1 al 8]

Al Presidente de la Universidad de Puerto Rico

2. Ver que el Rector de la UPRB cumpla con las **recomendaciones de la 3 a la 7** de este *Informe*. [Hallazgos del 1 al 8]

Al Rector de la Universidad de Puerto Rico en Bayamón

3. Asegurarse de que se realice y se documente un análisis de riesgos, según se establece en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. El informe, producto de este análisis de riesgos, debe ser remitido para revisión y aprobación. [Hallazgo 1]
4. Ejercer una supervisión efectiva sobre la Directora de la OSI para asegurarse de que:
 - a. En coordinación con el Decano de Asuntos Administrativos establezca las medidas necesarias para que se corrijan:
 - 1) Los problemas de filtraciones y humedad existentes en el Cuarto de Máquinas y se le provea mantenimiento continuo y preventivo a la planta generadora de electricidad. [Hallazgo 2-a.1)]
 - 2) Las deficiencias comentadas en el **Hallazgo 3-a.1) del a) al c) y e), y 2)b)**.
 - b. Realice las gestiones necesarias para que se adquieran baterías para los servidores, que provean la capacidad necesaria para efectuar los respaldos y bajar los sistemas de forma ordenada. [Hallazgo 2-a.1)b)]

- c. Establezca controles de seguridad físicos y ambientales adecuados para proteger los equipos de comunicaciones ubicados en los gabinetes, y sus respectivas conexiones. **[Hallazgo 3-a.1)d), 2)a) y c), y b.]**
 - d. Vea que el Especialista en Tecnologías de Comunicación I, ponga en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo del servidor para que:
 - 1) Requiera un mínimo de días para que el sistema le permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 4-a.1)a]**
 - 2) Defina un término fijo de intentos de acceso sin éxito a los recursos de la red para que el sistema deshabilite automáticamente las cuentas de acceso. **[Hallazgo 4-a.1)b]**
 - 3) Produzca un registro de auditoría de los eventos que se comentan en el **Hallazgo 4-a.2).**
 - e. Imparta instrucciones para que el personal asignado a revisar los registros del SIE mantenga la documentación de todas las revisiones efectuadas. Además, se asegure de impartir instrucciones para que se configure un registro de los accesos mediante conexiones remotas a los sistemas de información de la UPRB. **[Hallazgo 5]**
 - f. Se asegure de que el Director de Desarrollo de Tecnologías de Información de la OSI documente adecuadamente los procesos relacionados con el desarrollo y el cambio de aplicaciones. **[Hallazgo 7]**
5. Ver que el Decano de Asuntos Administrativos:
- a. Revise las *Normas y Procedimientos* para que requieran que las cerraduras de la OSI utilicen llaves distintas a las demás

instalaciones de la UPRB, y que el Oficial de Propiedad mantenga un registro por área que facilite obtener la información del personal que tiene llaves para acceder a la OSI. [Hallazgo 2-a.2)a) y d)]

b. Vea que el Oficial de Propiedad mantenga registros completos y actualizados sobre las autorizaciones y los recibos relacionados con la asignación de llaves al personal de la UPRB. [Hallazgo 2-a.2)b) y c)]

6. Evaluar y aprobar el *Plan de Contingencias OSI-UPRB* y las políticas, las normas y los procedimientos utilizados por la OSI que se comentan en el **Hallazgo 6**, y asegurarse de que los mismos se mantengan actualizados y se circulen al personal relacionado con estos.

7. Asegurarse de que se prepare un procedimiento que requiera al Especialista en Tecnologías de Comunicación I y a los administradores de las redes departamentales, que mantengan un registro actualizado de los servidores, y de los demás componentes de las redes a su cargo y su interconexión. Además, que requiera que los administradores departamentales envíen copia de estos registros a la Directora de la OSI. Este procedimiento debe ser remitido para revisión y aprobación. [Hallazgo 8]

AGRADECIMIENTO

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

Leticia del Contralor

Por: *Yennifer Maldonado*

ANEJO 1

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

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Ygrí Rivera de Martínez	Presidenta	27 jun. 09	16 dic. 09
Ing. Carlos H. del Río Rodríguez	Presidente	19 jun. 09	26 jun. 09
CPA Carlos J. Dávila Torres	Vicepresidente	28 jun. 09	16 dic. 09
Dr. Carlos I. Pesquera Morales	"	19 jun. 09	16 dic. 09
Dra. Rosa A. Franqui Rivera	Secretaria	21 oct. 09	16 dic. 09
Lcdo. Salvador Antonetti Zequeira	Secretario	19 jun. 09	5 oct. 09

ANEJO 2

UNIVERSIDAD DE PUERTO RICO EN BAYAMÓN
OFICINA DE SISTEMAS DE INFORMACIÓN
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Arturo Avilés González	Rector Interino	10 oct. 09	16 dic. 09
Prof. Irma Schmidt Soltero	Rectora	19 jun. 09	30 sep. 09
Sr. David González López	Decano de Asuntos Académicos Interino	1 oct. 09	16 dic. 09
Sr. Héctor De Jesús Cardona	Decano de Asuntos Académicos	19 jun. 09	30 sep. 09
Sr. Nelson Vázquez Espejo	Decano de Asuntos Estudiantiles Interino	1 sep. 09	16 dic. 09
Sra. Evangeline Medina Guarch	Decana de Asuntos Estudiantiles	19 jun. 09	11 ag. 09
Sr. Abdiel Martínez Barrios	Decano de Asuntos Administrativo Interino	20 oct. 09	16 dic. 09
Sr. Jorge Rovira Álvarez	"	19 jun. 09	19 oct. 09
Srta. Bárbara Landrau Espinosa	Directora de la Oficina de Sistemas de Información	19 jun. 09	16 dic. 09

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

**PRINCIPIOS PARA
LOGRAR UNA
ADMINISTRACIÓN
PÚBLICA DE
EXCELENCIA**

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-08-32* del 27 de junio de 2008, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensión 2124, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico Querellas@ocpr.gov.pr o a través de la página en Internet de la Oficina.

**INFORMACIÓN SOBRE
LOS INFORMES DE
AUDITORÍA**

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el Administrador de Documentos al (787) 294-0625 o (787) 200-7253, extensión 536.

**INFORMACIÓN DE
CONTACTO***Dirección física:*

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Internet:

<http://www.ocpr.gov.pr>

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069