Secretaría

Lcda. Tania Barbarossa Ortiz

- ☐ Ver al dorso
- ☐ Para su información
- ☐ Notas
- ☐ Para mantenerle al día
- ☐ Expediente
- ☑ Dar Cuenta
- ☐ Registrar y Procesar
- ☐ Archivar
- ☐ Preparar Carta

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

#855

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO SECRETARIA SENADO DE P.R.
2013 AUG -1 AM 9:57

8 de febrero de 2013

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Eduardo A. Bhatia Gautier
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-13-12* de la Oficina de Sistemas de Información del Recinto de Ciencias Médicas de la Universidad de Puerto Rico, aprobado por esta Oficina el 2 de febrero de 2013. Publicaremos dicho *Informe* en nuestra página en Internet: http://www.ocpr.gov.pr para conocimiento de los medios de comunicación y de otras partes interesadas.

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

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

Cordialmente,

Yesmín M. Valdivieso

Anejo

PO BOX 366069 SAN JUAN PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: http://www.ocpr.gov.pr

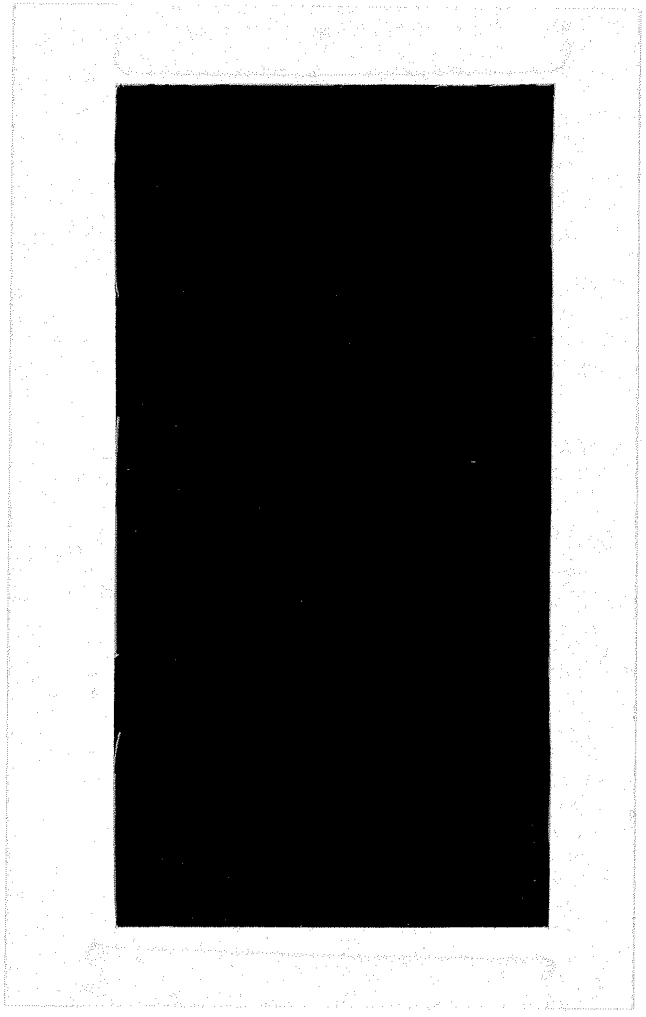
#855

COMPROMISO • INTEGRIDAD
TRANSPARENCIA

SENSIBILIDAD • JUSTICIA • EXCELENCIA

[redacted]

Estado Libre Asociado de Puerto Rico
Oficina del Contralor
San Juan, Puerto Rico



INFORME DE AUDITORÍA TI-13-12

2 de febrero de 2013

Universidad de Puerto Rico

Recinto de Ciencias Médicas

Oficina de Sistemas de Información

(Unidad 5510 - Auditoría 13532)

Período auditado: 20 de octubre de 2010 al 9 de junio de 2011

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **4**

OPINIÓN Y HALLAZGOS **5**

1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados del Recinto 5

2 - Falta de un plan de continuidad de negocios 7

3 - Falta de almacenamiento externo de los respaldos de datos del PPMI, y de un acuerdo para mantener un centro alterno para la recuperación de las operaciones 8

4 - Deficiencias relacionadas con los diagramas de las redes de área local del Recinto, y con el archivo donde se almacena la documentación de la configuración del equipo de telecomunicaciones conectado a la red de área amplia 10

5 - Deficiencias relacionadas con el control de acceso físico y los controles ambientales en los cuartos de distribución del cableado (*wiring closets*) del Recinto 13

6 - Falta de un inventario de las computadoras adquiridas por el Recinto y de un registro de programas instalados en cada una de estas 16

7 - Ausencia de una pantalla de advertencia sobre el uso de las computadoras del Recinto 19

RECOMENDACIONES **20**

AGRADECIMIENTO **23**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS DURANTE EL PERÍODO AUDITADO **24**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **25**

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

2 de febrero de 2013

Al Gobernador y a los presidentes del Senado
y de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) del Recinto de Ciencias Médicas (Recinto) de la Universidad de Puerto Rico (UPR), para determinar si 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 20 de octubre de 2010 al 9 de junio de 2011. 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; inspección física; y análisis de documentos y de otra información pertinente.

CONTENIDO DEL INFORME

Este es el primer informe, y contiene siete hallazgos sobre el resultado de del examen que realizamos de los controles para la administración del programa de seguridad, la continuidad del servicio, el acceso físico y la red de comunicaciones. El mismo está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

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. El 16 de junio de 1993 se aprobó la *Ley 16-1993*, la cual enmendó el Artículo 3 de la *Ley Núm. 1*, eliminó el Consejo de Educación Superior como cuerpo rector de la UPR y creó la Junta de Síndicos. Esta gobierna y administra el Sistema Universitario de Puerto Rico, incluido el Recinto.

El Recinto tiene como misión formar los recursos humanos que fomentarán y mantendrán las mejores condiciones de salud del pueblo puertorriqueño, en tres dimensiones: la educación, la investigación y el servicio. Al Recinto se le concedió autonomía académica y administrativa dentro de las normas que se disponen en la *Ley Núm. 1*, y las que se fijen en el *Reglamento General de la Universidad* o en las resoluciones de la Junta de Síndicos.

La dirección administrativa y académica del Recinto la ejerce un Rector, el cual es nominado por el Presidente de la UPR previa consulta de este al Senado Académico para ser nombrado por la Junta de Síndicos. El Rector ejercerá la autoridad administrativa y académica dentro del ámbito de su respectiva unidad institucional, conforme a lo dispuesto en la *Ley*, y en las normas y los reglamentos universitarios.

Cada una de las unidades del Sistema Universitario tiene una Junta Administrativa integrada por el Rector; los decanos de asuntos académicos, estudiantiles y administrativos; los decanos de facultad; los directores de departamentos académicos; el Senado Académico; y un estudiante electo anualmente. El Rector será el Presidente de la mencionada Junta Administrativa.

El Recinto se compone de las siguientes facultades: Medicina, Odontología, Salud Pública, Farmacia, Enfermería y Colegio de Profesionales relacionados con la Salud. Además, cuenta con la Oficina del Rector y con tres decanatos de apoyo: Administración, Estudiantes y Asuntos Académicos.

La OSI es responsable de velar por el buen funcionamiento del servidor que contiene las aplicaciones administrativas del Recinto. Estas son: *Student Information System* (SIS) y *Human Resource System* (HRS), entre otras. Además, la OSI se encarga de mantener la infraestructura de la red de comunicaciones, la cual brinda servicios a los tres decanatos y a las seis facultades. No obstante, los decanatos y las facultades cuentan con sus propios recursos tecnológicos y aplicaciones, los cuales son administrados por personal técnico asignado a los mismos. La OSI está adscrita a la Oficina del Rector y es dirigida por una Directora.

Los fondos para financiar las actividades operacionales del Recinto provienen, principalmente, de asignaciones legislativas, aportaciones federales e ingresos que genera de sus actividades. Para los años fiscales 2009-10 y 2010-11, el Recinto incurrió en gastos operacionales de $326,087,492 y $306,233,658. De estos, $1,031,791 y $927,544, correspondían al presupuesto operacional asignado a la OSI para los años fiscales 2009-10 y 2010-11.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta y de los funcionarios principales del Recinto que actuaron durante el período auditado.

El Recinto cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.rcm.upr.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. Rafael Rodríguez Mercado, Rector, mediante carta de nuestros auditores del 9 de junio de 2011. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 1 de julio de 2011, el Rector remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados al redactar el borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Rector para comentarios, por carta del 11 de septiembre de 2012. El 26 de septiembre de 2012 el Rector solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 27 de septiembre de 2012 le concedimos al Rector la prórroga solicitada hasta el 12 de octubre de 2012.

El Rector contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 10 de octubre de 2012. Sus comentarios se consideraron en la redacción final de este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas y la evidencia en nuestro poder demuestran que las operaciones relacionadas con los sistemas de información de la OSI del Recinto, en lo que concierne a los controles para la administración del programa de seguridad, la continuidad del servicio, el acceso físico, y la red de comunicaciones, no se realizaron conforme a las normas generalmente aceptadas en este campo. A continuación se comentan los **hallazgos del 1 al 7**.

Hallazgo 1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados del Recinto

Situación

a. Un análisis de riesgos de los sistemas de información computadorizados 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 y pertinentes a las operaciones de la entidad gubernamental, y respondan a las posibles amenazas identificadas. El análisis 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.

El Recinto contaba con la OSI que tenía a cargo el centro de cómputos, la red de comunicaciones y los sistemas administrativos principales. Además, contaba con personal encargado de administrar y salvaguardar aplicaciones y equipos computadorizados localizados en sus tres decanatos y seis facultades. Este personal le respondía a los decanos y a los a directores de las facultades.

Al 9 de mayo de 2011, el Recinto no había preparado un informe de análisis de riesgos, que cumpliera con los objetivos mencionados e incluyera todos sus 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 al Recinto evaluar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de este, y considerar cómo protegerlos para reducir los riesgos de daños materiales y de pérdida de información.

Causa

La situación comentada se atribuye a que el Rector no promulgó una directriz para la preparación y la documentación de un análisis de riesgos, según lo establecido en la *Carta Circular Núm. 77-05*, que incluyera todos los sistemas de información del Recinto.

Comentarios de la Gerencia

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

> Desde febrero de 2003, el Recinto cuenta con un Oficial de Seguridad y Cumplimiento, desde junio de 2004 cuenta con un Plan de Contingencia de Sistemas de Información, desde abril de 2005 cuenta con una Política de Seguridad de Tecnologías de Información del RCM, en todos ellos está implícito el análisis de riesgo [...] [*sic*]

Consideramos las alegaciones del Rector, pero determinamos que el **Hallazgo** prevalece porque el plan y la política a las que hace referencia en su contestación no incluyen información que permita cumplir con los objetivos de un análisis de riesgos.

Véanse las recomendaciones de la 1 a la 3.

Hallazgo 2 - Falta de un plan de continuidad de negocios

Situación

a. Al 9 de mayo de 2011, el Recinto no tenía un plan de continuidad de negocios que incluyera un plan de continuidad de operaciones y un plan de recuperación de desastres. En su lugar, contaban con el *Plan de Contingencia* de la OSI (*Plan*), el cual proveía para la restauración de los sistemas administrativos del Recinto, pero no proveía para la recuperación de las operaciones computadorizadas realizadas en los tres decanatos y las seis facultades.

   El plan de continuidad de negocios es necesario para restaurar las operaciones y lograr el pronto funcionamiento de las operaciones críticas del Recinto en caso de riesgos tales como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

Criterio

La situación comentada es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

Efecto

La situación comentada podría propiciar la improvisación y, que en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios que presta el Recinto a sus usuarios.

Causa

La situación comentada se atribuye a que faltaba un análisis de riesgos de los sistemas de información computadorizados del Recinto (Véase el **Hallazgo 1**) que sirviera de base para el plan de continuidad de negocios.

Véanse las recomendaciones 1, 2 y 4.

Hallazgo 3 - Falta de almacenamiento externo de los respaldos de datos del PPMI, y de un acuerdo para mantener un centro alterno para la recuperación de las operaciones

Situaciones

a. El Plan de Práctica Médica Intramural (PPMI) es un programa adscrito a la Facultad de Medicina del Recinto. El PPMI administra los servicios médicos universitarios que se ofrecen a un costo razonable a través de los hospitales adscritos y de los afiliados al Recinto[1]. En el año fiscal 2009-10, la facturación de estos servicios ascendió a $66,146,558[2].

   El examen realizado el 3 de junio de 2011 sobre los respaldos de los datos de la facturación de servicios médicos que ofrece el PPMI, reveló que estos no se almacenaban en un lugar externo, fuera de los servidores[3] donde se realizaban los mismos.

---

[1] Los nombres de los hospitales se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector para comentarios.

[2] Estos se consideran fondos públicos.

[3] Los nombres de los servidores se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector para comentarios.

b. Al 3 de junio de 2011, la facultad de Medicina del Recinto no contaba con un centro alterno para restaurar las operaciones críticas del PPMI en caso de emergencia. Tampoco había formalizado acuerdos escritos con otra entidad para establecer un centro alterno en las instalaciones de esta.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establece que deberán existir procedimientos para tener y mantener una copia de respaldo recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones de la entidad.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del plan de continuidad de negocios, 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. El propósito es recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. **[Apartado a.]** Además, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes:

- un centro alterno de la propia entidad
- una entidad pública o privada de similar configuración y tamaño
- una compañía dedicada a servicios de restauración. **[Apartado b.]**

Efectos

La situación comentada en el **apartado a.** puede ocasionar que, en casos de emergencias, el PPMI no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

La situación comentada en el **apartado b.** podría afectar las funciones del Recinto y los servicios provistos por el PPMI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales del PPMI.

Causa

Las situaciones comentadas se deben a que el plan de contingencias del PPMI se encontraba en proceso de diseño y aún se evaluaban alternativas para el almacenamiento externo de los respaldos y para el establecimiento del centro alterno.

Véanse las recomendaciones 1, 2 y 5.

Hallazgo 4 - Deficiencias relacionadas con los diagramas de las redes de área local del Recinto, y con el archivo donde se almacena la documentación de la configuración del equipo de telecomunicaciones conectado a la red de área amplia

Situaciones

a. El 4 de marzo de 2011 la División de Telecomunicaciones (DT) de la OSI contaba con un diagrama lógico de la red de área amplia[4] (*WAN*, por sus siglas en inglés) que incluía los componentes principales de esta e identificaba las 43 redes de área local[5] (*LAN*, por sus siglas en inglés). La DT proveyó a nuestros auditores los diagramas correspondientes a 20 de las 43 redes de área local. El examen realizado a estos diagramas reveló que carecían de la siguiente información importante:

- La descripción de la distribución por piso y del equipo de comunicaciones ubicado en los cuartos de distribución de cableado

[4] Es una red de comunicación que se conecta con diferentes lugares remotos que puede incluir desde distancias cortas, como por ejemplo un piso o un edificio, hasta transmisiones extremadamente largas que abarcan una región grande o varios países.

[5] Es una red de comunicación que sirve a varios usuarios dentro de un área geográfica específica.

- La configuración básica del equipo de comunicación (nombre e *IP Address*[6])
- Las interconexiones del equipo a través de los *switches*[7], el *firewall*, y los *routers* y el cableado vertical (*backbone*), instalados en el edificio principal y en la biblioteca
- El detalle de los servidores, incluidos los destinados para el monitoreo de la red y los puntos de acceso inalámbricos, con sus respectivas identificaciones y localizaciones
- El detalle de las computadoras e impresoras conectadas a la red con sus respectivas identificaciones y localizaciones.

b. Al 28 de abril de 2011 el archivo[8] utilizado para el respaldo de la documentación de la red carecía de información relacionada con las instalaciones, las interconexiones y las configuraciones de todos los equipos de telecomunicaciones conectados a la red de área amplia del Recinto, tales como: impresoras, *módems* y *routers*, entre otros. En su lugar, el archivo sólo incluía la documentación correspondiente a la configuración de 15 de los 250 (6%) equipos de telecomunicaciones existentes.

Criterios

Las situaciones comentadas se apartan de lo establecido en la Sección VII del *Procedimiento de Trabajo División de Telecomunicaciones*, aprobado el 4 de marzo de 2011 por la Directora de la OSI. En este se establece que el personal de telecomunicaciones mantendrá la documentación de los diagramas de la red de comunicación del Recinto. Toda esta documentación se mantendrá en un servidor de archivos y se revisará periódicamente cuando sea necesario.

---

[6] Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

[7] Dispositivo de comunicación central para líneas de comunicaciones de red que permite que ocurran transmisiones simultáneas, y aumenta el ancho de banda de la red.

[8] El nombre y el lugar de almacenaje de este archivo se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector 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 de los equipos 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.

Efectos

Las situaciones comentadas impiden al Recinto tener una compresión clara y precisa de los componentes de la red, y dificulta mantener control eficiente y efectivo en la administración y en el mantenimiento a la misma. Además, dificulta la atención de problemas de conexión en un tiempo razonable y que se planifique efectivamente las mejoras a la red, según el crecimiento de sus sistemas.

Causa

Las situaciones comentadas se atribuyen a que la Directora de la OSI no se aseguró de que los empleados de la DT actualizaran periódicamente la documentación relacionada con la red de comunicaciones del Recinto, según el crecimiento de su infraestructura.

Comentarios de la Gerencia

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

> Desde la última Auditoria de la Oficina de Sistemas de Información (OSI) del RCM realizada por el Contralor en 1994, los equipos de telecomunicaciones de la red de comunicación del RCM han tenido un crecimiento exponencial dado que de un ambiente centralizado sin cuartos de comunicación hemos evolucionado a uno descentralizado con [...] Evolucionando la División de Telecomunicaciones de 2 empleados (en el 1994) a 3 en la actualidad para atender toda esta infraestructura de comunicación. [*sic*]

Véanse las recomendaciones 1, 2, y 6.a. y b.

Hallazgo 5 - Deficiencias relacionadas con el control de acceso físico y los controles ambientales en los cuartos de distribución del cableado (*wiring closets*) del Recinto

Situaciones

a. La red de comunicaciones del Recinto interconecta los recursos de computación utilizados por todos sus usuarios. El equipo principal de comunicación está ubicado en el Centro de Cómputos de la OSI bajo la responsabilidad de la DT. El equipo de comunicaciones restante se encuentra en cuartos de cableado (*wiring closets*) y en gabinetes localizados en varios edificios del Recinto.

1) En el examen realizado en el Recinto el 29 de marzo y el 1 de abril de 2011 relacionado con el control de acceso físico existente en 14 cuartos[9] de distribución de cableado y en 7 gabinetes[10], se identificaron las siguientes deficiencias:

a) Ninguno de los cuartos de distribución del cableado tenía un diagrama de los *drops*[11]. Además, los cables no estaban amarrados ni organizados. Tampoco estaban identificados al ser conectados a los *switches*, desde el panel de distribución (*Patch Panel*).

b) Cuatro cuartos de distribución de cableado y dos gabinetes fueron ubicados en áreas donde estaba localizado el panel del servicio telefónico. Además, un gabinete fue ubicado en un cuarto de máquinas de acondicionadores de aire y otro en un baño.

c) El *switch* del Programa de Subvencionados de la División de Administración Financiera, que administra los fondos federales de las investigaciones del Recinto, estaba

---

[9] La localización de los cuartos se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector para comentarios.

[10] La localización de los gabinetes se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Rector para comentarios.

[11] Conector de pared para las instalaciones de redes.

localizado fuera de un gabinete. Además, estaba conectado a un generador de energía ininterrumpible (*UPS*, por sus siglas en inglés) que no funcionaba.

d) La Administración de los programas ACTU y Pediátrico Hemofilia, y la Oficina de Seguridad del Recinto eran los custodios de las llaves de cinco cuartos de cableado localizados en varios edificios del Recinto. Por esto, el personal de la OSI no tenía control ni libre acceso a los mismos para atender cualquier eventualidad que afectara las operaciones de la red.

e) Un cuarto de distribución de cableado y cinco gabinetes permanecían abiertos. Además, dos gabinetes tenían las llaves puestas.

2) Con relación a los controles ambientales examinados en 15 cuartos de distribución de cableado y 5 gabinetes, se determinó lo siguiente:

a) El equipo de telecomunicaciones instalado en 14 cuartos de distribución de cableado y en 3 gabinetes tenían polvo acumulado.

b) En 11 cuartos de distribución de cableado y en las áreas donde estaban ubicados 2 gabinetes no había acondicionadores de aire, por lo que la temperatura existente en los mismos no era adecuada.

c) Seis cuartos de distribución de cableado y un gabinete carecían de iluminación en su interior para facilitar el mantenimiento a los equipos.

d) Dos cuartos de distribución de cableado y las áreas donde estaban ubicados dos gabinetes eran utilizados para almacenar materiales y otros equipos, tales como: cajas de cartón, documentos, equipos de computadoras y una escalera de aluminio.

e) Dos cuartos de distribución de cableado no contaban con un extintor cerca del lugar.

f) Un gabinete estaba localizado debajo de una tubería de agua que tenía filtración.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la Sección VIII.B.8 de la *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, aprobada mediante la *Certificación Núm. 35* del 19 de febrero de 2008 por la Junta de Síndicos. En esta se establece que cada OSI tiene la responsabilidad de proveerle recursos de tecnología de información a los usuarios que tienen una necesidad legítima; y al mismo tiempo, de proteger las redes, los sistemas y los datos de la Universidad del acceso no autorizado y del abuso.

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

- se controle adecuadamente el acceso a las áreas donde están ubicados los equipos de comunicaciones **[Apartado a.1)]**
- se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas. **[Apartado a.2)]**

Efectos

La situación comentada en el **apartado a.1)a)** impide a la DT de la OSI 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 de la misma. Además, dificulta atender los 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) del b) al e)** pueden propiciar que personas ajenas a las operaciones de la red causen daños al equipo por error o intención, lo que podría afectar adversamente el funcionamiento de la red y la continuidad de las operaciones.

Las situaciones comentadas en el **apartado a.2)** podrían poner en riesgo la seguridad de los empleados y de los recursos sensitivos de los sistemas computadorizados. Además, podrían impedir la disponibilidad de los sistemas y, por consiguiente, limitar los servicios que presta el Recinto.

Causa

Las situaciones comentadas se deben a que el Rector no se aseguró de que el Director de Recursos Físicos del Recinto corrigiera las situaciones mencionadas y atendiera las solicitudes de servicio y de mantenimiento que había realizado la Directora de la OSI.

Véanse las recomendaciones 1, 2, 6.c. y 7.

Hallazgo 6 - Falta de un inventario de las computadoras adquiridas por el Recinto y de un registro de programas instalados en cada una de estas

Situaciones

a. Al 4 de marzo de 2011, el Recinto no mantenía lo siguiente:

   1) Un inventario de las computadoras adquiridas por la Rectoría, las facultades y los decanatos del Recinto que incluyera, entre otras cosas, la descripción, el custodio, el número de propiedad, la fecha de adquisición, el precio unitario y la localización de las mismas.

   2) Un registro de los programas adquiridos e instalados en cada una de las computadoras del Recinto que incluyera, entre otras cosas, el número de licencia de los programas instalados; el nombre

del usuario; el número de propiedad y la descripción de la computadora donde estaban instalados los programas; y el costo de los mismos.

Una situación similar se comentó en el *Informe de Auditoría CPED-94-10*.

Criterios

La situación comentada en el **apartado a.1)** es contraria a lo establecido en el *Reglamento para el Control de la Propiedad Mueble de la Universidad de Puerto Rico*, aprobado mediante la *Certificación Núm. 62* del 19 de agosto de 1994 por la Junta de Síndicos. En dicho Reglamento 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. **[Artículo VI.C.]**
- Numerar físicamente el activo y registrarlo en los expedientes. **[Artículo VIII.E.]**
- Hacer pruebas para determinar la confiabilidad del proceso de inventario antes de proceder con la certificación final del inventario. **[Artículo IX.D.]**

Además, es norma de sana administración y de control interno que las entidades mantengan registros de la propiedad confiables y actualizados. Esto permite ejercer un control eficaz de los activos, asegurar que los mismos existan y fijar responsabilidades a los empleados que tienen a su cargo la custodia de la propiedad, en caso de alguna situación irregular. **[Apartado a.1)]**

La situación comentada en el **apartado a.2)** es contraria a lo establecido en el *Procedimiento para la Adquisición, Instalación, Conservación y Uso Oficial de los Programas en Computadoras de la Universidad de Puerto Rico*[12], aprobado el 12 de enero de 2001 por el Presidente de la UPR. En este se establece que:

- La OSI será responsable de la administración y la conservación de los programas y sus licencias **[Sección IV.H]**.
- El director de cada oficina designará un empleado que será responsable de mantener un inventario que incluya lo siguiente: el nombre del producto, la versión, el nombre del manufacturero, la orden de compra o evidencia de adquisición y el número de la propiedad en el cual está instalado. **[Sección VIII.A.2]**
- La OSI conservará en un lugar seguro el conjunto de discos compactos u otros medios donde se registran los programas de soluciones a nivel sistémico, propiedad de la unidad. **[Sección VIII.B]**

Efectos

Las situaciones comentadas impiden al Recinto ejercer un control adecuado sobre la propiedad, los programas y las licencias correspondientes. Esto podría propiciar el uso indebido o la pérdida del equipo computadorizado, así como la instalación y el uso de programas no autorizados, sin que estas situaciones puedan detectarse a tiempo para fijar responsabilidades. También dificulta nuestra gestión fiscalizadora.

Causas

La situación comentada en el **apartado a.1)** se atribuye a que no se requirió, desde la adquisición e implementación de la aplicación utilizada para el registro de la propiedad, la identificación del equipo computadorizado en el campo *category*.

---

[12] Este *Procedimiento* fue revisado el 4 de agosto de 2011, bajo el título *Procedimiento de la Oficina de Sistemas de Información de la Administración Central para Utilizar y Administrar Programas de Computadoras.* El mismo contiene disposiciones similares a las del procedimiento aprobado en el 2001.

La situación comentada en el **apartado a.2)** se debe a que la Directora de la OSI, los decanos y los directores de las facultades no cumplieron con las disposiciones reglamentarias citadas. Esto, con el propósito de proteger y salvaguardar la seguridad de los recursos de informática, y así cumplir con la responsabilidad compartida sobre estos recursos.

Véanse las recomendaciones 1, 2, 8 y 9.a.

Hallazgo 7 - Ausencia de una pantalla de advertencia sobre el uso de las computadoras del Recinto

Situación

a. Al 7 de abril de 2011, cuatro[13] (67%) de seis computadoras del Recinto examinadas al azar[14] no incluían una advertencia en la pantalla inicial para notificar a los usuarios sobre las normas principales para el uso de las mismas.

Criterios

La situación comentada es contraria a lo establecido en la Sección 3.3 de la *Política de Seguridad de Tecnología de Información del RCM.* En esta se establece que el objetivo principal de la OSI es establecer y promulgar políticas, guías, procedimientos y estándares de tecnologías de información que faciliten y promuevan el uso de estas en forma integrada, para satisfacer las necesidades de los usuarios del Recinto. Además, es contraria a lo establecido en la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la *Carta Circular Núm. 77-05.* En esta se establece, entre otras cosas, que cada entidad gubernamental debe colocar un aviso que indique al usuario, o a quien acceda a su sistema de información, que el mismo es propiedad de esa entidad del Estado Libre Asociado de Puerto Rico, y que se compromete a utilizarlo conforme a las normas establecidas.

---

[13] Los números de propiedad o de serie de las computadoras se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Rector para comentarios.

[14] Al 4 de marzo de 2011, la Oficina de Propiedad y la OSI no pudieron proveer para nuestro examen un inventario del equipo computadorizado.

Efectos

La falta de la pantalla de advertencias en las computadoras del Recinto puede dar lugar a que los usuarios no observen las normas principales para el uso de los sistemas de información, y a que se dificulte imponer sanciones por la violación a las mismas. Además, puede provocar la comisión de irregularidades y otras situaciones adversas.

Causa

La situación comentada se debe a que los decanos y los directores de facultades, en coordinación con la Directora de la OSI, no se aseguraron de que las advertencias fueran instaladas en todas las computadoras del Recinto como control efectivo para asegurarse del uso oficial de los sistemas computadorizados.

Véanse las recomendaciones 1, 2 y 9.b.

RECOMENDACIONES

A la Junta de Síndicos de la Universidad de Puerto Rico

1. Ver que el Presidente de la Universidad de Puerto Rico cumpla con la **Recomendación 2** de este *Informe*. **[Hallazgos del 1 al 7]**

Al Presidente de la Universidad de Puerto Rico

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

Al Rector del Recinto de Ciencias Médicas

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*, que incluya todos los sistemas de información del Recinto. El informe producto de este análisis de riesgos debe ser remitido para su revisión y aprobación. **[Hallazgo 1]**

4. Asegurarse de que se prepare un *Plan de Continuidad de Negocios* que integre todos los sistemas de información del Recinto, o que las áreas que no cuentan con sus planes de contingencia preparen y documenten los mismos, y los remitan a la OSI para su integración con el *Plan de Contingencia* de la OSI. Además, asegurarse de que el

plan o los planes se remitan para su consideración y aprobación, se prueben periódicamente y se divulguen a los empleados y a los funcionarios concernientes. **[Hallazgo 2]**

5. Asegurarse de que en el plan de contingencias del PPMI se considere:

   a. Almacenar el respaldo de los datos de la facturación de servicios médicos que ofrece el PPMI en un lugar externo. **[Hallazgo 3-a.]**

   b. Establecer un centro alterno a las instalaciones físicas del PPMI, que no esté expuesto a los mismos riesgos, o se formalice un acuerdo escrito con otra entidad que acepte la utilización de los equipos del PPMI en casos de desastres o emergencias. **[Hallazgo 3-b.]**

6. Ejercer una supervisión eficaz sobre la Directora de la OSI para que se asegure de que el Director de la DT:

   a. Prepare un diagrama esquemático de la red del Recinto que incluya los aspectos mencionados en el **Hallazgo 4-a.** Además, revise periódicamente el mismo para mantenerlo actualizado.

   b. Mantenga en el archivo utilizado para el respaldo de la documentación de la red, la información completa y actualizada de los componentes de la misma y de su configuración. Además, produzca una copia de este archivo para respaldo externo. **[Hallazgo 4-b.]**

   c. Identifique, amarre y organice el cableado horizontal, de manera que se prepare un diagrama de los *drops*. Una vez preparado, incluyan copia de este en un área visible en los cuartos de distribución del cableado. **[Hallazgo 5-a.1)a)]**

7. Impartir instrucciones al Director de Recursos Físicos del Recinto para que, en coordinación con la Directora de la OSI, se asegure de que se establezcan las medidas necesarias para:

   a. La protección física de los equipos de la red, de manera que no estén accesibles al personal ajeno a las operaciones de esta. **[Hallazgo 5-a.1) del b) al e)]**

   b. La corrección de las deficiencias de control ambiental comentadas en el **Hallazgo 5-a.2)**.

8. Ejercer una supervisión eficaz sobre el Decano de Administración para asegurarse de que el Encargado de Propiedad del Recinto realice las gestiones necesarias para corregir la identificación del equipo computadorizado en la aplicación utilizada para el registro de la propiedad. **[Hallazgo 6-a.1)]**

9. Impartir instrucciones a la Directora de la OSI, a los decanos y a los directores de facultades para que:

   a. Mantengan un registro de los programas computadorizados del Recinto. El registro deberá contener, entre otra información, el número de las licencias de los programas disponibles e instalados en las computadoras, el nombre del usuario, el número de propiedad y la descripción de la computadora donde están instalados los mismos. **[Hallazgo 6-a.2)]**

   b. Se aseguren de que toda computadora en el Recinto incluya una advertencia en la pantalla inicial que notifique a los usuarios sobre las normas principales para el uso de la misma, de que se informen las medidas aplicables en caso de violación de dichas normas y de que los usuarios se comprometan a observar las mismas. **[Hallazgo 7]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yamis M Valdivieso

ANEJO 1

UNIVERSIDAD DE PUERTO RICO
RECINTO DE CIENCIAS MÉDICAS
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	20 oct. 10	9 jun. 11
CPA Carlos J. Dávila Torres	Vicepresidente	20 oct. 10	9 jun. 11
Lcdo. Luis Berríos Amadeo	Segundo Vicepresidente	20 oct. 10	9 jun. 11
Prof. Aida Ávalo de Sánchez	Secretaria	20 oct. 10	9 jun. 11

ANEJO 2

UNIVERSIDAD DE PUERTO RICO
RECINTO DE CIENCIAS MÉDICAS
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Rafael Rodríguez Mercado	Rector	20 oct. 10	9 jun. 11
Dra. Lyvia Álvarez Pagán	Ayudante Ejecutiva	20 oct. 10	9 jun. 11
Dr. Pedro Santiago Borrero	Decano Interino Escuela de Medicina	16 ene. 11	9 jun. 11
Dr. Walter R. Frontera Roura	Decano de la Escuela de Medicina	20 oct. 10	15 ene. 11
Sr. Eleuterio Pomales Garay	Decano de Administración	20 oct. 10	9 jun. 11
Sr. Efraín Piñero Medina	Director Ejecutivo PPMI	20 oct. 10	9 jun. 11
Sra. Maribel Hernández Iglesias	Directora de Finanzas	20 oct. 10	9 jun. 11
Prof. Sandra Santos Nieves	Directora Oficina de Sistemas de Información	20 oct. 10	9 jun. 11

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 mediante 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

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

http://www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr