

16034



Secretaria
Wadelein

- 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 Leves



[Handwritten initials]

Iniciales

Oficina del Presidente

Katherine Erazo

CHIEF OF STAFF

Fecha

29 junio de 2012

Referido a

Madelaine Rivera

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



OFICINA DEL PRESIDENTE
HON. THOMAS RIVERA SCHATZ

HOJA DE TRÁMITE

Fecha referido 30 DE JUNIO DE 2012

Referido a SRA. MADELINE RIVERA
SUB-SECRETARIA

De *Margie Huertas*
MARGIE HUERTAS
SECRETARIA

Asunto **INFORME ANUAL DE LA OFICINA DEL COMISIONADO DE SEGUROS DE PR 2011 Y
COPIA DEL INFORME DE AUDITORÍA T1-12-12 DE LA OFICINA DE SISTEMAS DE
INFORMACIÓN DEL SISTEMA DE RETIRO DE LA UPR.**

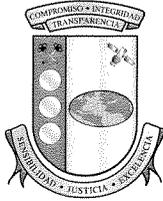
- Para su conocimiento
 Para acción correspondiente
 Para trabajar y contestar directamente
 Autorizado

OBSERVACIONES

Recibido por _____ Fecha _____ Hora _____

RECIBIDO SECRETARIA
SENADO DE P.R.
2012 JUN 30 PM 1:43





Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

29 de junio de 2012

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

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

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-12-12* de la Oficina de Sistemas de Información del Sistema de Retiro de la Universidad de Puerto Rico, aprobado por esta Oficina el 26 de junio de 2012. Publicaremos dicho *Informe* en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

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

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

Cordialmente,


Yesmín M. Valdivieso

Anejo

RECIBIDO SECRETARIA
SENADO DE P.R.
2012 JUN 30 PM 1:43

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ
2012 JUN 29 PM 2:43

0-18963



INFORME DE AUDITORÍA TI-12-12

26 de junio de 2012

Sistema de Retiro de la Universidad de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5531 - Auditoría 13444)

Período auditado: 12 de abril al 15 de octubre de 2010



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 de los sistemas de información computadorizados	5
2 - Falta de un plan de seguridad	7
3 - Falta de un plan de continuidad de negocios, y de un acuerdo escrito con un centro alternativo para la continuidad de las operaciones	9
4 - Falta de configuración de la política de auditoría en el sistema operativo del servidor principal del Sistema de Retiro	11
5 - Falta de documentación de las solicitudes de cambio, y deficiencias en las formas OSI-108	12
6 - Falta de normas y de procedimientos para reglamentar las operaciones de la OSI, de documentación de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad, y de aprobación de la documentación creada para la nueva programación.....	15
7 - Falta de información en las etiquetas que identificaban los respaldos de información.....	18
8 - Falta de adiestramientos relacionados con la administración de las cuentas y la seguridad de los sistemas, el desarrollo y el control de cambios, y con la atención de situaciones de emergencia en la OSI	20
RECOMENDACIONES	21
AGRADECIMIENTO	24
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS DURANTE EL PERÍODO AUDITADO	25
ANEJO 2- FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	26

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

26 de junio 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) del Sistema de Retiro de la Universidad de Puerto Rico (Sistema de Retiro), para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Efectuamos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

**ALCANCE Y
METODOLOGÍA**

La auditoría cubrió del 12 de abril al 15 de octubre de 2010. 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 el resultado del examen de los controles relacionados con la administración del programa de seguridad, el desarrollo y el control de los cambios de las aplicaciones, y la continuidad del servicio. El mismo está disponible en nuestra página en Internet: <http://www.ocpr.gov.pr>.

**INFORMACIÓN SOBRE
LA UNIDAD AUDITADA**

El Sistema de Retiro se creó por disposición de la *Ley Núm. 135 del 7 de mayo de 1942*. Esta *Ley* fue derogada por la *Ley Núm. 1 del 20 de enero de 1966, Ley de la Universidad de Puerto Rico*, creada para reorganizar la estructura funcional de la Universidad.

Mediante la *Ley 16-1993*, se enmendó el Artículo 3 de la *Ley Núm. 1* para eliminar el Consejo de Educación Superior como cuerpo rector de la Universidad y crear la Junta de Síndicos (Junta). Esta gobierna y administra el sistema público universitario de Puerto Rico, incluido el Sistema de Retiro. 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, elegidos por representantes del personal docente y del estudiantado en la Junta Universitaria.

La Junta es el fiduciario del fondo de pensiones y, como tal, es la responsable del funcionamiento adecuado del Sistema de Retiro. La Junta es quien único tiene autoridad legal para aprobar la reglamentación del Sistema de Retiro en cuanto a los derechos y a las obligaciones tanto de los empleados participantes, como de la Universidad como patrono. La Junta es nombrada por el Gobernador con el consejo y el consentimiento del Senado.

El Sistema de Retiro se rige por las disposiciones de la *Certificación Núm. 27 del 14 de septiembre de 1973*, según enmendada. En esta *Certificación* se aprobó una resolución para reorganizar el Sistema de Retiro y su reglamento. El propósito del Sistema de Retiro es proveer beneficios a los funcionarios y a los empleados de la Universidad contra los riesgos de edad avanzada, incapacidad, muerte o cesantía, con el objetivo de promover a personas idóneas a entrar y permanecer en el servicio de esta y contribuir a una administración eficiente. El Sistema de Retiro se considera una unidad administrativa de la Junta.

Las funciones ejecutivas del Sistema de Retiro las ejerce un Director Ejecutivo, quien es nombrado por la Junta. Las operaciones diarias del Sistema de Retiro consisten en orientar a los participantes, efectuar el trámite de toda solicitud de préstamos y de beneficios de pensión, contabilizar toda transacción que se origine, y mantener los expedientes de los participantes. Para llevar a cabo estas funciones, cuenta con las secciones de Contabilidad, Beneficios, Pensiones, y Préstamos, y con la OSI. Estas responden a la oficina del Director Ejecutivo.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta de Síndicos y de los funcionarios principales del Sistema de Retiro que actuaron del 12 de abril al 15 de octubre de 2010, respectivamente.

La OSI es dirigida por un Director de Sistemas de Información y cuenta con dos especialistas de sistemas de información y un Programador en Sistemas Electrónicos I. Los recursos tecnológicos que utiliza el Sistema de Retiro están distribuidos entre las instalaciones físicas de este y las de la Administración Central de la Universidad de Puerto Rico (AC).

Los recursos para el funcionamiento del Sistema de Retiro provienen de tres fuentes principales: la aportación patronal, la aportación de sus miembros y las inversiones. Para los años fiscales del 2007-08 al 2009-10, el presupuesto operacional asignado al Sistema de Retiro ascendió a \$9,188,495, \$9,643,952 y \$8,507,689, respectivamente. El presupuesto asignado para las operaciones de la OSI para los años fiscales del 2007-08 al 2009-10 fue de \$544,856, \$529,875 y \$255,000, respectivamente¹.

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

¹ La reducción en el presupuesto asignado a los sistemas de información entre los años fiscales del 2007-08 al 2009-10 obedecía a que en los primeros dos años se solicitó un presupuesto para implantar un sistema de información, el cual finalmente se determinó no establecer.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Sr. José A. Lázaro Nazario, Director Ejecutivo del Sistema de Retiro, mediante carta de nuestros auditores del 7 de octubre de 2010.

Mediante carta del 26 de octubre de 2010, el Director Ejecutivo remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Director Ejecutivo, para comentarios, por carta del 1 de febrero de 2012.

El Director Ejecutivo contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 15 de febrero de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a la administración del programa de seguridad, el desarrollo y el control de los cambios de las aplicaciones, y la continuidad del servicio no se realizaron conforme a las normas generalmente aceptadas en este campo. A continuación se comentan los **hallazgos del 1 al 8**.

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

Situación

- a. Un avalúo 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 y se determina 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 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 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 26 de agosto de 2010, en el Sistema de Retiro no se había realizado un avalúo de riesgos de 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.

Efectos

La situación comentada impide al Sistema de Retiro estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de este, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificulta desarrollar un *Plan de Continuidad de Negocios* donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Sistema de Retiro en caso de que surja alguna eventualidad. [Véase el Hallazgo 3]

Causa

La situación comentada se atribuye a que el Director Ejecutivo no había promulgado una directriz para la preparación y la documentación del avalúo de riesgos de los sistemas de información del Sistema de Retiro, según se establece en la *Carta Circular Núm. 77-05*.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

Se está solicitando al Director de Sistemas de Información que prepare un Informe de Avalúo de Riesgos que señale los procedimientos para evaluar la seguridad de los sistemas de información. Este documento se utilizará para realizar Valuaciones de Riesgo anualmente. Para el análisis de riesgo se tendrá que mantener un inventario de activos de sistemas de información que incluyen el equipo y los programas. El inventario debe estar clasificado de acuerdo al nivel de importancia para la continuidad de las operaciones. El informe incluirá un balance en el impacto económico entre el impacto de las amenazas y las medidas de seguridad a implantarse. [sic]

Véanse las recomendaciones 1 y 3.

Hallazgo 2 - Falta de un plan de seguridad**Situación**

- a. Al 6 de mayo de 2010, el Sistema de Retiro no tenía un plan de seguridad aprobado por el Director Ejecutivo, que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad²
 - La evidencia de un análisis de riesgo actualizado, que sea la base del plan de seguridad
 - La responsabilidad de la gerencia, y de los demás componentes de la unidad
 - Un programa de adiestramiento especializado al equipo clave de seguridad

² La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el avalúo de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas, el personal de sistemas de información y los usuarios, y el cual permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

Criterios

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

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con este. Los mismos deben considerar los sistemas y las instalaciones principales, e identificar los deberes de los dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas.

Efectos

La falta de un plan de seguridad podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

Causa

La situación comentada se atribuye a que el Director Ejecutivo no había promulgado una directriz para la preparación del plan de seguridad.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

El Director de Sistemas de Información preparará un Plan de Seguridad, diseñado a base del Informe de Avalúo de Riesgos dirigido a proteger el personal, equipos y datos del Sistema de Retiro. [sic]

Véanse las recomendaciones 1 y 4.

Hallazgo 3 - Falta de un plan de continuidad de negocios, y de un acuerdo escrito con un centro alternativo para la continuidad de las operaciones

Situaciones

- a. Al 20 de septiembre de 2010, el Sistema de Retiro carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la OSI. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la OSI en caso de riesgos, tales como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros. En su lugar, el Sistema de Retiro utiliza el *Plan de Contingencia de la Oficina de Sistemas de Información de Administración Central para la Continuidad del Servicio ante Emergencias (Plan de Contingencia)*, el cual no incluye una descripción de los recursos tecnológicos ni de los procesos del Sistema de Retiro para la recuperación de sus operaciones.
- b. Al 5 de octubre de 2010, el Sistema de Retiro no había formalizado acuerdos con otra entidad para establecer un centro alternativo en las instalaciones de esta, que permita restaurar las operaciones críticas computadorizadas en casos de emergencia.

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*.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del *Plan de Continuidad de Negocios*, 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: **[Apartado b.]**

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración

- Un centro alternativo de la propia entidad.

Efectos

La situación comentada en el **apartado a.** 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 a los usuarios del Sistema de Retiro.

La situación comentada en el **apartado b.** podría afectar las funciones del Sistema de Retiro y los servicios de la OSI, 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 de la OSI.

Causa

Las situaciones comentadas se atribuyen a que el Director de la OSI no había requerido la preparación de un plan de continuidad de negocios para el Sistema de Retiro ni la identificación de un centro alternativo para utilizarlo en caso de emergencia. Esto, porque entendía que estas eran actividades propias de la Oficina de Sistemas de Información de la AC.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

Una vez desarrollado el Informe de Avalúo de Riesgos el Director de Sistemas de Información coordinará con la oficina de Sistemas de Información de la Administración Central de la Universidad de Puerto Rico, para que dentro de su Plan de Contingencia, se incorpore activamente al Sistema de Retiro y se incluya descripción de los recursos tecnológicos y de los procesos propios para la recuperación de las operaciones del Sistema de Retiro. Las operaciones informáticas vitales del Sistema de Retiro se desarrollan en equipo de computación ubicado y propiedad de la Administración Central. Se formalizará un acuerdo con otra unidad de la Universidad de Puerto Rico para restaurar operaciones críticas computadorizadas en casos de emergencia y utilizar la misma como centro alternativo. [*sic*]

Véanse las recomendaciones 1, 5.a. y 6.

Hallazgo 4 - Falta de configuración de la política de auditoría en el sistema operativo del servidor principal del Sistema de Retiro

Situación

- a. El examen efectuado el 10 de mayo de 2010 sobre los parámetros de seguridad configurados en el sistema operativo del servidor principal del Sistema de Retiro reveló que no se había activado la política de auditoría (*Audit Policy*) para que el sistema produjera un registro de los siguientes eventos:
- Las solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*)
 - La creación, la modificación o la eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)
 - La administración de los directorios de servicio (*Directory service management*)
 - Los accesos a los archivos, cartapacios (*folders*) e impresoras (*Audit object access*)
 - Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)
 - El uso de los privilegios de los usuarios (*Audit privilege use*)
 - Las acciones ejecutadas de los procesos (*Audit process tracking*)
 - El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*)

Criterio

La situación comentada se aparta de lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

Efectos

La situación comentada impide la detección temprana de errores críticos o problemas con los servidores, que permita tomar de inmediato las medidas preventivas y correctivas necesarias. Además, priva a la gerencia de las herramientas necesarias para supervisar eficientemente los trabajos realizados por los usuarios, y detectar el acceso y uso indebido de los sistemas computadorizados.

Causa

La situación comentada se debía, en parte, a que el Director de la OSI entendía que activar las opciones de seguridad provistas por el sistema operativo que permitían examinar periódicamente los registros de seguridad, afectaría la capacidad de espacio y de procesamiento del servidor principal.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

Se activaran los "Audit Policy" necesarios y que estén disponibles en el servidor principal [...] del Sistema de Retiro. El servidor [...] actual del Sistema de Retiro no tiene la capacidad en espacio (disco duro) y procesamiento para manejar estos requerimientos. Recientemente se han adquirido nuevos servidores para actualizar los anteriores, los mismos tienen la capacidad para manejar los requerimientos indicados. Al día de hoy la OSI se encuentra en el proceso de instalación y configuración de los mismos. [sic]

Véanse las recomendaciones 1 y 5.b.

Hallazgo 5 - Falta de documentación de las solicitudes de cambio, y deficiencias en las formas OSI-108**Situación**

- a. El proceso de control de cambios a los programas de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad del Sistema de Retiro se inicia cuando los peticionarios solicitan, mediante correo electrónico, una modificación en la programación al Director de la OSI. Este asigna las modificaciones al Programador en Sistemas Electrónicos I o a las Especialistas en Sistemas de Información, quienes son responsables de efectuar los cambios en la programación. Para esto, acceden a un directorio de prueba, creado en el servidor

localizado en la AC. Primero, obtienen una copia del programa en producción. Segundo, generan una copia de la versión original del programa. Finalmente, se produce un archivo con las diferencias.

Para documentar y controlar las solicitudes de cambio, la OSI y la Unidad de Operaciones de la AC utilizan la *Forma OSI-108, Solicitud de Trabajo para el Área de Operaciones (Forma OSI-108)*. Una vez se efectúa una modificación a un programa, el Director de la OSI envía por correo electrónico la *Forma OSI-108* a la Unidad de Operaciones de la AC para documentar la ejecución de los cambios correspondientes. El registro de las peticiones de cambio y el seguimiento a las mismas se mantienen a través del registro *Track It*.

El examen de la documentación relacionada con 25 solicitudes de cambio del registro *Track It*, reveló lo siguiente:

- 1) El Director de la OSI no proveyó para examen de nuestros auditores lo siguiente:
 - a) Las formas *OSI-108* correspondientes a 20 solicitudes de cambio
 - b) La documentación de las pruebas y de la aceptación de los usuarios de los 25 cambios realizados.
- 2) Una de las Especialistas en Sistemas de Información no pudo suministrar para el examen de nuestros auditores la siguiente documentación:
 - a) Copia del programa en producción, previo a los cambios realizados en la programación relacionados con 16 solicitudes de cambio³
 - b) Copia de la versión del programa en producción, afectado por 15 solicitudes de cambio³

³ Las solicitudes de cambio se incluyeron en el borrador de los **hallazgos** de este *Informe*, remitido al Director Ejecutivo para comentarios.

- c) Copia del programa en producción, luego de realizados los cambios relacionados con 15 solicitudes⁴.
- 3) Las formas *OSI-108* provistas por la AC, y que habían sido tramitadas por la OSI del Sistema de Retiro, revelaron las siguientes deficiencias:
- a) Las 25 solicitudes no tenían la firma de autorización de la OSI para que la AC procediera con la ejecución del cambio.
 - b) Siete solicitudes no incluían el nombre ni la firma del programador o de la especialista que efectuó el cambio.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular Núm. 77-05*. [Apartado a.]

Las situaciones comentadas en el **apartado a.1) y 2)** son contrarias a lo establecido en la *Política Núm. TIG-003* de la mencionada *Carta Circular*.

La situación comentada en el **Apartado a.3)a)** es contraria a lo establecido en la Sección 5.2.2, *Método para Cambios en Programación Existente*, del *Manual de Normas de Documentación*, aprobado el 21 de abril de 2009 por la Vicepresidenta en Investigación y Tecnología de la Administración Central de la Universidad de Puerto Rico.

Efectos

Las situaciones comentadas dificultan mantener un control adecuado de los cambios realizados a la programación de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad del Sistema de Retiro.

La situación comentada en el **apartado a.3)** podría propiciar que se efectúen cambios no autorizados en el sistema, lo que constituye un riesgo adicional para su buen funcionamiento y para la integridad de la información contenida en el mismo. Además, propicia el ambiente para la comisión de errores e irregularidades.

⁴ Véase la nota al calce 3.

Causa

Las situaciones comentadas se debían, en parte, a que el Director del OSI no había preparado un procedimiento para el desarrollo y el control de los cambios, que requiriese, entre otras cosas, completar en todas sus partes la *Forma OSI-108*, u otra similar, y mantener la documentación completa y correcta de las modificaciones efectuadas a los programas de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

Se adquirió una nueva versión del programa "Track- IT", la cual se instalará en uno de los nuevos servidores adquiridos (tienen capacidad para manejar el programa) y aquí se archivarán los registros de las solicitudes de servicios que los usuarios hacen a la OSI. Se establecerá un procedimiento escrito para establecer todo lo relacionado con los procesos de cambios y manejos de las aplicaciones críticas del Sistema de Retiro. No se podrá realizar ningún cambio a los programas y/o archivos sin la solicitud y autorización de la oficina dueña de los datos y la aprobación del Director de la Oficina de Sistema de Información en la Forma OSI-108. También tendrán que archivar estas acompañadas de documentación que evidencie las pruebas efectuadas y la aceptación de los usuarios. [sic]

Véanse las recomendaciones 1, y 5.c.1) y 2).

Hallazgo 6 - Falta de normas y de procedimientos para reglamentar las operaciones de la OSI, de documentación de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad, y de aprobación de la documentación creada para la nueva programación

Situaciones

- a. Al 19 de mayo de 2010, no se habían establecido las normas y los procedimientos necesarios para reglamentar los siguientes procesos de la OSI:
 - La configuración, la administración y la documentación de los servidores
 - La administración de las cuentas creadas en el servidor principal del Sistema de Retiro

- La producción y la revisión de los registros de eventos de los servidores
 - La administración de la seguridad física de la OSI, y del cuarto de servidores y de telecomunicaciones
 - El proceso de respaldo, y la utilización, el almacenamiento y la disposición de las cintas o medios magnéticos y digitales
 - El desarrollo y el control de cambios de las aplicaciones, y el movimiento de programas entre las librerías
 - La autorización y la documentación de los cambios de emergencia efectuados a las aplicaciones
 - La investigación, la documentación y el manejo de incidentes no esperados.
- b. Al 19 de mayo de 2010, el Sistema de Retiro no mantenía un diagrama de flujo, un diccionario de datos ni un manual de programas, entre otros, como documentación de los módulos de Pensiones, Beneficios, Préstamos y Contabilidad. Estos módulos fueron puestos en producción hace más de 15 años.
- c. Entre enero de 2001 y febrero de 2010, una Especialista en Sistemas de Información I se había encargado de documentar los procesos creados en programación nueva, tal como *SQL* y *Visual Basic*, los cuales interactuaban con los módulos de Pensiones, Beneficios, Préstamos y Contabilidad. La documentación desarrollada consistía de 14 manuales de sistemas, 13 manuales de usuarios y 4 procesos. El examen de la mencionada documentación, reveló las siguientes deficiencias:
- 1) Al 21 de julio de 2010, la documentación desarrollada no estaba aprobada por el Director de la OSI ni por el Director Ejecutivo del Sistema de Retiro.

- 2) Al 13 de septiembre de 2010, 6 usuarios responsables de ejercer 8 de los 13 procesos documentados por la Especialista en los manuales de usuarios, desconocían de la existencia de los mismos.

Situaciones similares a las indicadas en los **apartados a. y b.** se comentaron en el *Informe de Auditoría Interna OAIC-2007-07* del 6 de junio de 2007.

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*.

Las situaciones comentadas en los **apartados b. y c.** son contrarias a lo establecido en la *Política Núm. TIG-011* de la indicada *Carta Circular*.

Las normas generalmente aceptadas en el campo de la tecnología de información sugieren que las entidades deben mantener una documentación completa y actualizada de los sistemas en producción. Una documentación adecuada del funcionamiento de un sistema computadorizado y sus programas provee información esencial para la implantación y la operación eficaz de este. Esta es de utilidad para el desarrollo de programas complementarios y es fuente de información para el estudio y la evaluación de los controles internos y para el adiestramiento del personal nuevo.

Efectos

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

Causas

Las situaciones comentadas en los **apartados a. y b.** obedecen, principalmente, a que el Director de la OSI no había desarrollado y

remitido para la consideración y aprobación del Director Ejecutivo, las normas y los procedimientos escritos para regular los procesos ni la documentación de sistemas necesaria, que se indican en estos apartados.

Las situaciones comentadas en el **apartado c.** obedecían a que el Director de la OSI no había remitido a la consideración del Director Ejecutivo los procedimientos preparados por la Especialista en Sistemas de Información I, para aprobación y divulgación.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

Se está solicitando al Director de Sistemas de Información que desarrolle y le someta al Director Ejecutivo para su consideración y aprobación las normas y procedimientos que se tendrían que establecer para las problemáticas presentadas en este Hallazgo, se trabajará en la creación de las normas y procedimientos considerando el impacto que podría tener este proceso en los servicios que ofrece la Oficina de Sistemas de Información. [sic]

Véanse las recomendaciones 1, y 5.d.1) y e.

Hallazgo 7 - Falta de información en las etiquetas que identificaban los respaldos de información

Situación

- a. La Unidad de Operaciones de la AC era responsable de preparar los respaldos diarios, semanales, mensuales y anuales de la información mantenida en sus servidores. En estos se incluía el respaldo de los datos procesados por los módulos de Pensiones, Beneficios, Préstamos y Contabilidad utilizados por el Sistema de Retiro. El respaldo original se mantenía en gabinetes arrendados por la AC en un centro de respaldo externo, y copia del mismo se conservaba en una bóveda.

El Programador en Sistemas Electrónicos I era responsable de preparar y de mantener en su oficina el respaldo semanal del servidor principal del Sistema de Retiro. El respaldo contenía, entre otros, todas las transacciones ejecutadas en el Sistema de Retiro, incluidos

los cambios a las aplicaciones, los cambios en los privilegios asignados a los usuarios, y la configuración de la red y de los servidores.

Las inspecciones realizadas el 18 de agosto y el 14 de septiembre de 2010 a las etiquetas de los respaldos de información relacionados con los datos del Sistema de Retiro, los cuales se mantenían en la oficina del programador y en el centro de respaldo externo, respectivamente, revelaron que estas carecían de la siguiente información:

- La descripción clara de los archivos respaldados
- La identificación de la procedencia de los archivos
- El tamaño del respaldo
- El lugar asignado para su almacenamiento.

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 priva al Sistema de Retiro de mantener un control adecuado de las cintas de respaldos, lo que podría afectar la continuidad de las operaciones debido a la pérdida de información importante, con los consiguientes efectos adversos.

Causa

La situación comentada se debía a que el personal de la OSI no contaba con procedimientos aprobados para la preparación y el control de los respaldos.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

La Oficina de Sistemas de Información creará los procedimientos que permitan la preparación, manejo e identificación de los resguardos indicados. [*sic*]

Véanse las recomendaciones 1, y 5.c.3) y d.2).

Hallazgo 8 - Falta de adiestramientos relacionados con la administración de las cuentas y la seguridad de los sistemas, el desarrollo y el control de cambios, y con la atención de situaciones de emergencia en la OSI

Situaciones

- a. El personal de la OSI es responsable, entre otras cosas, de administrar la seguridad, dar mantenimiento a sus siete servidores, efectuar los cambios a la programación y garantizar la continuidad de las operaciones del Sistema de Retiro. El Director de la OSI autoriza y crea las cuentas de acceso en la Red, y los directores de las secciones de Pensiones, Beneficios, Préstamos y Contabilidad asignan los privilegios otorgados a los usuarios de sus módulos.

Mediante entrevistas realizadas a los directores de estas secciones, y el examen de la documentación de adiestramientos tomados por el personal de la OSI y los mencionados directores, determinamos lo siguiente:

- 1) Al 23 de abril de 2010, el personal de la OSI del Sistema de Retiro no había sido adiestrado para ejecutar procedimientos de emergencia.
- 2) Al 18 de agosto de 2010:
 - a) El Programador de Sistemas Electrónicos I no había participado en adiestramientos relacionados con el desarrollo y el control de cambios de las aplicaciones.
 - b) Los Especialistas en Sistemas de Información y el Director de la OSI no habían recibido adiestramientos relacionados con la programación durante los últimos 35 meses.
 - c) El Director de la OSI no había tomado adiestramientos relacionados con la administración de la seguridad de los sistemas de información.
- 3) Al 9 de septiembre de 2010, los directores no habían recibido adiestramientos relacionados con las funciones de seguridad que tenían a su cargo.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

Efecto

Las situaciones comentadas podrían afectar la seguridad de los sistemas de información, exponer los datos a riesgos innecesarios como la pérdida de información almacenada, y afectar la continuidad de las operaciones.

Causa

Las situaciones comentadas se debían, en parte, a que el Director Ejecutivo no le había requerido al Director de la OSI que, en coordinación con la Directora de Recursos Humanos de la AC, efectuara un estudio sobre las necesidades de adiestramientos relacionados con los sistemas de información, para los funcionarios y los empleados del Sistema de Retiro y que, conforme al estudio, se asegurara de que el personal recibiera los adiestramientos mencionados.

Comentarios de la Gerencia

En la carta del Director Ejecutivo, este nos indicó lo siguiente:

El Sistema de Retiro coordinará con la Oficina de Recursos Humanos de la Administración Central la elaboración de un estudio para identificar las necesidades de adiestramientos sobre informática que necesita el personal de la Oficina de Sistemas de Información. Luego se trabajará con este estudio para proveer al personal de OSI los adiestramientos necesarios. [sic]

Véanse las recomendaciones 1, 2 y 5.f.

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

1. Ver que el Director Ejecutivo del Sistema de Retiro cumpla con las recomendaciones de la 3 a la 6 de este *Informe*. [Hallazgos del 1 al 8]
2. Ver que la Oficina de Recursos Humanos de la AC, en coordinación con el Director de la OSI, realice el estudio de necesidades de adiestramiento que se requiere en la **Recomendación 5.f.** de este *Informe*. [Hallazgo 8]

Al Director Ejecutivo del Sistema de Retiro de la Universidad de Puerto Rico

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. Una vez aprobado, ver que se revise anualmente para asegurarse de que se mantiene actualizado.

[Hallazgo 1]

4. Realizar las gestiones necesarias para que el Sistema de Retiro cuente con un *Plan de Seguridad* que incluya los criterios descritos en el **Hallazgo 2**. Además, se asegure de que se realicen pruebas periódicas al *Plan de Seguridad*, y que el mismo se divulgue a los empleados y a los funcionarios concernientes.

5. Ejercer una supervisión eficaz sobre el Director de la OSI para asegurarse de que:

- a. Prepare y remita para su consideración y aprobación un *Plan de Continuidad de Negocios*, que incluya un *Plan de Recuperación de Desastres* y un *Plan para la Continuidad de las Operaciones*. Una vez el *Plan* sea revisado y aprobado, asegurarse de que se realicen pruebas periódicas y se divulgue a los empleados y a los funcionarios concernientes. Además, se mantenga copia del mismo en un lugar seguro fuera del Sistema de Retiro.

[Hallazgo 3-a.]

- b. Active las opciones contenidas en la pantalla de políticas de auditorías (*Audit Policies*) que se mencionan en el **Hallazgo 4**.

- c. Tome las medidas necesarias para que:

- 1) Se mantenga la documentación completa de los cambios realizados a los programas y de las pruebas efectuadas a estos, antes de ser transferidos al ambiente de producción.

[Hallazgo 5-a.1) y 2)]

- 2) Se complete en todas sus partes y se incluyan todas las firmas requeridas en la *Forma OSI-108*, según se indica en el apartado a.3) del **Hallazgo 5**.
 - 3) Se incluya en las etiquetas de los respaldos la información indicada en el **Hallazgo 7**.
- d. Prepare y remita para su consideración y aprobación, las normas y los procedimientos necesarios para:
- 1) Reglamentar las operaciones que se indican en el **Hallazgo 6-a**.
 - 2) Preparar y controlar los respaldos de información. **[Hallazgo 7]**
- e. Prepare, revise y mantenga actualizada la documentación relacionada con los módulos de Pensiones, Beneficios, Préstamos y Contabilidad que se incluye en el **Hallazgo 6-b. y c**. Una vez esta sea preparada, remita para aprobación, y se asegure de que la misma sea distribuida a los empleados y a los funcionarios concernientes.
- f. Efectúe, en coordinación con la Directora de la Oficina de Recursos Humanos de la AC, un estudio sobre las necesidades de adiestramientos de los funcionarios que tienen a su cargo la seguridad de los sistemas de información del Sistema de Retiro, y las de los empleados de la OSI, y velar por que se ofrezcan, entre otros, los adiestramientos que se mencionan en el **Hallazgo 8**.
6. Formalizar un acuerdo escrito con un centro alternativo que acepte la utilización de sus respectivos equipos en caso de desastres o emergencias en la OSI, o considerar establecer su propio centro alternativo en alguna de las instalaciones de la Universidad de Puerto Rico que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 3-b.]**

AGRADECIMIENTO

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

Oficina del Contralor

Por:

Yermis M. Valdivia

ANEJO 1

SISTEMA DE RETIRO DE LA UNIVERSIDAD DE PUERTO RICO
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	12 abr. 10	15 oct. 10
CPA Carlos Dávila Torres	Vicepresidente	12 abr. 10	15 oct. 10
Prof. Aida Ávalo de Sánchez	Secretaria	29 ag. 10	15 oct. 10
Dra. Rosa A. Franqui Rivera	"	12 abr. 10	30 jun. 10

ANEJO 2

SISTEMA DE RETIRO DE LA UNIVERSIDAD DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. José A. Lázaro Nazario	Director Ejecutivo	12 abr. 10	15 oct. 10
Sr. Willie Rosario Arroyo	Subdirector	12 abr. 10	15 oct. 10
Sr. Carlos López Rivera	Director de Sistemas de Información	12 abr. 10	15 oct. 10



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

Internet:

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

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069
San Juan, Puerto Rico 00936-6069