

Principales Datos
24/sep/2012



Secretaría

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

Senado
DE PUERTO RICO

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

T: 787.722.3460
787.722.4012
F: 787.723.5413
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

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

COMISIONES ESPECIALES

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

COMISIONES CONJUNTAS

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



[Handwritten initials]

Iniciales

Oficina del Presidente

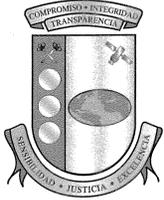
Katherine Erazo

CHIEF OF STAFF

Fecha 19 de septiembre 2010

Referido a Durilda Ortiz

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



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso

Contralora

19 de septiembre 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 copias de los informes de auditoría *TI-13-05* y *TI-13-06* de la División de Tecnologías Académicas y Administrativas del Recinto de Río Piedras de la Universidad de Puerto Rico y de la Oficina de Tecnología de Información de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura, respectivamente, aprobados por esta Oficina el 12 de septiembre de 2012. Publicaremos dichos informes 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,

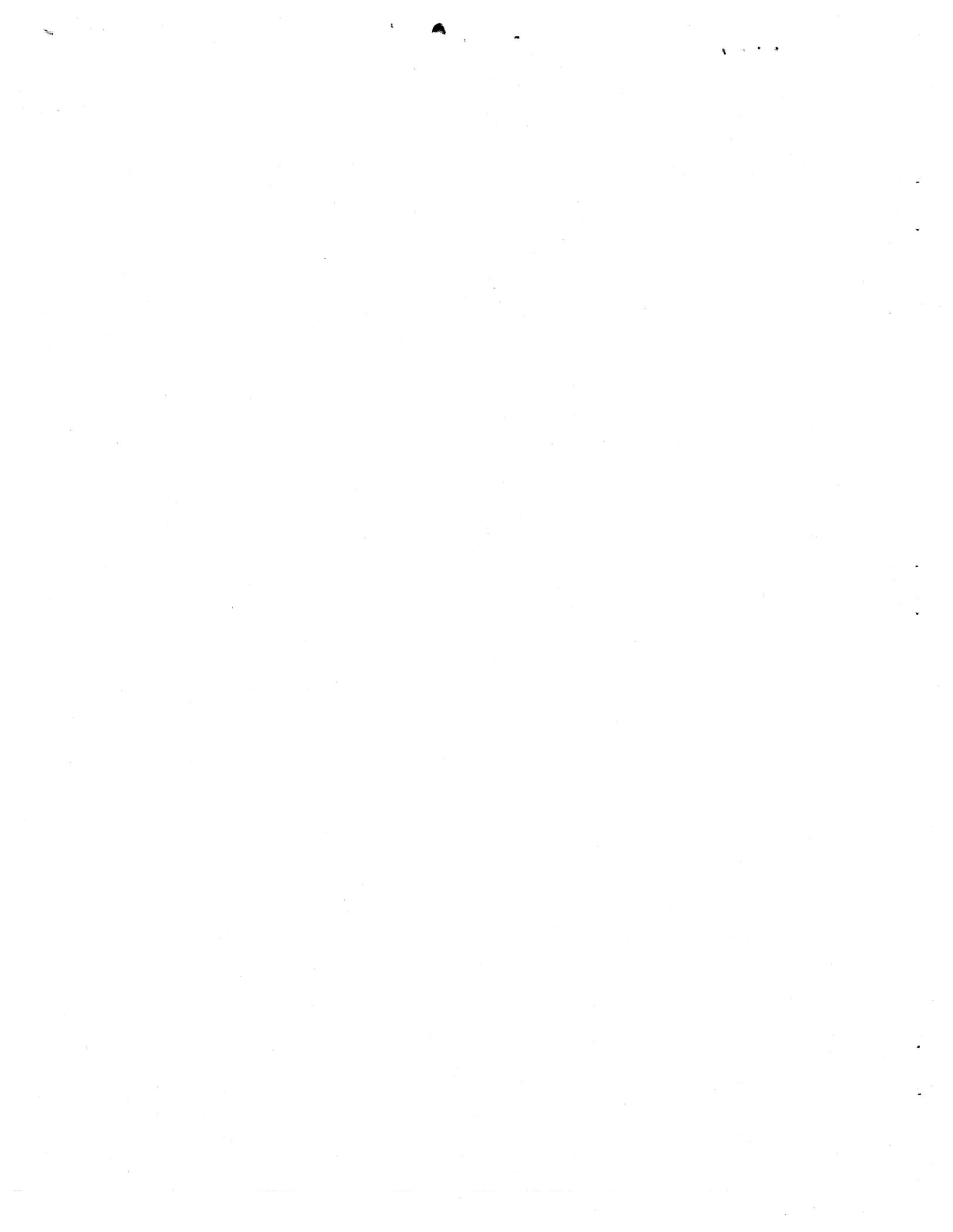

Yesmín M. Valdivieso

Anejos

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ
2012 SEP 19 AM 10:34

4100413

210741



INFORME DE AUDITORÍA TI-13-05

12 de septiembre de 2012

Universidad de Puerto Rico

Recinto de Río Piedras

División de Tecnologías Académicas y Administrativas

(Unidad 5530 - Auditoría 13301)

Período auditado: 22 de mayo de 2009 al 17 de mayo de 2010

CONTENIDO

	Página
ALCANCE Y METODOLOGÍA	2
CONTENIDO DEL INFORME	2
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	2
COMUNICACIÓN CON LA GERENCIA	4
OPINIÓN Y HALLAZGOS	4
1 - Falta de informes de análisis de riesgos de los sistemas de información computadorizados, y deficiencias en el de la DTAA y en los de las áreas de servicios técnicos	4
2 - Falta de planes de seguridad sobre los sistemas de información del Recinto	8
3 - Deficiencias en el Plan de Contingencia de la División de Tecnologías Académicas y Administrativas, y falta de pruebas o simulacros para comprobar su efectividad	10
4 - Deficiencias en los parámetros relacionados con las políticas de auditoría de los servidores	12
5 - Deficiencias relacionadas con el acceso físico a los cuartos de distribución de cableado y con los estantes en los que se encontraban los equipos de comunicación.....	14
6 - Deficiencias relacionadas con el almacenamiento de los respaldos de los archivos computadorizados de información	17
7 - Procedimientos sin aprobar por la Rectora del Recinto	19
8 - Falta de controles adecuados de los formularios de cheques en blanco, y de los discos compactos que contiene las firmas autorizadas para pago	20
9 - Falta de documentación relacionada con la justificación y la autorización de los accesos a las cuentas con privilegios de administrador, y del otorgamiento de privilegios de conexión remota a los sistemas de información.....	22
10 - Falta de revisiones periódicas de los registros de auditoría producidos por el sistema y de los accesos a Internet.....	23
RECOMENDACIONES	25
AGRADECIMIENTO	28
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS DURANTE EL PERÍODO AUDITADO	29
ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	30

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

12 de septiembre 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 División de Tecnologías Académicas y Administrativas (DTAA) del Recinto de Río Piedras de la Universidad de Puerto Rico (Recinto) para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control establecido para el procesamiento de 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 22 de mayo de 2009 al 17 de mayo de 2010. 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 diez hallazgos sobre el resultado del examen que realizamos de los controles de acceso lógico y físico, y sobre aspectos de seguridad y continuidad del servicio.

**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 Universidad de Puerto Rico (UPR). En la misma se establece que

la UPR tiene como misión esencial alcanzar los objetivos de transmitir e incrementar el saber por medio de las ciencias y de las artes, ponerlo al servicio de la comunidad a través de la acción de sus profesores, investigadores, estudiantes y egresados, y contribuir al cultivo y disfrute de los valores éticos y estéticos de la cultura.

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. Mediante la *Ley 65-2010* se enmendó este Artículo, a los fines de ampliar la composición de los miembros de la Junta de Síndicos. 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 UPR, 2 son profesores y 1 estudiante. Los profesores y el estudiante son elegidos por representantes del personal docente y del estudiantado en la Junta Universitaria, respectivamente.

La administración y la supervisión de las operaciones del Recinto las ejerce un Rector nominado por el Presidente de la UPR, previa consulta de este al Senado Académico, para ser nombrado por la Junta de Síndicos. El Rector preside la Junta Administrativa y el Senado Académico.

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

La estructura organizacional del Recinto está compuesta por una Oficina de Rectoría a la cual están adscritos el Senado Académico, la Junta Administrativa, la Junta de Disciplina, 4 decanatos, 6 facultades, 2 escuelas, 7 oficinas administrativas, la División de Seguridad, el Teatro, el Museo, el Instituto de Estudios Hostosianos y la DTAA.

Los recursos del Recinto provienen de asignaciones legislativas, fondos federales, donativos e ingresos propios. Para el año fiscal 2009-10, el presupuesto asignado al Recinto fue de \$239,564,000.

El Recinto cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.uprrp.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 a la Dra. Ana R. Guadalupe Quiñones, entonces Rectora Interina del Recinto, por carta de nuestros auditores, del 12 de agosto de 2010.

Mediante carta del 20 de septiembre de 2010, la doctora Guadalupe Quiñones remitió sus comentarios sobre 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 a la doctora Guadalupe Quiñones, Rectora del Recinto, y a la Dra. Gladys Escalona De Motta, ex-Rectora del Recinto, para comentarios, por cartas del 13 de enero de 2012.

La Rectora contestó el borrador de los **hallazgos** de este *Informe* por carta del 30 de enero de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*. La ex-Rectora no contestó el borrador de los **hallazgos** de este *Informe* que le fuera remitido para comentarios por carta del 13 de enero de 2012, y mediante carta de seguimiento del 1 de febrero de 2012.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la DTAA en lo que concierne a los controles de acceso lógico y físico, y los aspectos de la seguridad 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 10**.

Hallazgo 1 - Falta de informes de análisis de riesgos de los sistemas de información computadorizados, y deficiencias en el de la DTAA y en los de las áreas de servicios técnicos

Situaciones

- a. Un análisis de riesgos¹ 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

¹ Al análisis de riesgos también se le conoce como avalúo de riesgos.

identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El 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 DTAA que tenía el centro de cómputos principal y mantenía sus sistemas administrativos principales. Además, contaba con 17 áreas de servicios técnicos, las cuales no le respondían a la DTAA. Estas tenían personal encargado de administrar y salvaguardar los equipos computadorizados, y los correspondientes centros de cómputos que mantenían las diferentes escuelas, facultades, divisiones, oficinas administrativas y decanatos.

Nuestro examen sobre la existencia de un informe de análisis de riesgos reveló que:

- 1) El Recinto no había preparado un informe de análisis de riesgos que incluyera todos sus sistemas de información. En su lugar, se prepararon 15 informes individuales para 14 áreas y la DTAA. Además, el personal encargado de administrar y

salvaguardar los equipos computadorizados de las restantes 3 áreas² no había preparado el referido informe de análisis de riesgos.

- 2) En los 15 informes de análisis de riesgos que nos fueron provistos, encontramos las siguientes deficiencias³:
 - a) Los informes no incluían una lista del inventario de los activos de sistemas de información. Diez informes (67 por ciento) no contenían una descripción de los equipos computadorizados principales, 12 (80 por ciento) no tenían información sobre las aplicaciones instaladas en los sistemas y los 15 (100 por ciento) no tenían información sobre interfaces con otros sistemas de información ni sobre los datos que mantienen los sistemas y su nivel de criticidad.
 - b) Los informes no identificaban las posibles amenazas y vulnerabilidades lógicas y físicas que podrían afectar los activos de sistemas de información del Recinto, ni la probabilidad de que ocurran esas amenazas. En los 15 informes no se habían identificado las posibles amenazas, y en 13 (87 por ciento) no se habían identificado las vulnerabilidades de los activos de sistemas de información.
 - c) No se realizó un análisis del impacto sobre las operaciones del Recinto en caso de que se materialice alguna amenaza. Trece informes no contenían el nivel de probabilidad de que la amenaza se presentara y los 15 no contenían el nivel de la magnitud del impacto sobre los activos de sistemas de información.

² Los nombres de las áreas se incluyeron en el borrador de los **hallazgos** del *Informe* remitido a la Rectora y a la ex-Rectora del Recinto para comentarios.

³ La relación de los informes y de las deficiencias identificadas en los mismos se incluyó en el borrador de los **hallazgos** del *Informe* remitido a la Rectora y a la ex-Rectora del Recinto para comentarios.

- d) Los informes no incluían información sobre las medidas de control establecidas para proteger cada uno de los activos de sistemas de información y determinar si los controles existentes para mitigar el riesgo eran eficaces. Cuatro informes (27 por ciento) no contenían información sobre los controles establecidos, y los 15 no contenían información sobre los que se planifican implantar para reducir los riesgos a los que están expuestos los activos de sistemas de información.

Criterio

Las situaciones comentadas son contrarias 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

Las situaciones comentadas impiden al Recinto evaluar 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 de pérdida de información.

Causa

Las situaciones comentadas se atribuyen a que la Rectora no había promulgado 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 de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Se reclutará a un Oficial de Manejo de Riesgos, en un término de tres meses, quién diseñará un Cuestionario de Avalúo de Riesgos de Tecnología para el Recinto incluyendo los objetivos señalados en el inciso 2.a. Se le dará prioridad a esta iniciativa dentro del plan de trabajo anual, 2012-2013. Se designarán oficiales de

enlace en cada Facultad quienes serán adiestrados para que realicen esta evaluación. Se incluirá en el plan de 2011-2014 un itinerario para la ejecución del avalúo de riesgos en las facultades. [sic] [Apartado a.1)]

El nuevo Cuestionario de Avalúo de Riesgos de la DTAA para el Recinto requerirá un inventario de los activos de sistemas de información. Este inventario contendrá la descripción de los equipos principales, información sobre las aplicaciones instaladas, interfaces con otros sistemas, tipo de información almacenada y su nivel de criticidad. [sic] [Apartado a.2)a)]

El nuevo Cuestionario de Avalúo de Riesgos proveerá una guía para identificar las posibles amenazas y vulnerabilidades lógicas y físicas que podrían afectar los activos de información. [sic] [Apartado a.2)b)]

El nuevo Cuestionario de Avalúo de Riesgos incluirá herramientas para un análisis de impacto en las operaciones en caso de que se materialice alguna amenaza, nivel de probabilidad de que ocurra y nivel de magnitud del impacto sobre los activos y sistemas de información. [sic] [Apartado a.2)c)]

El nuevo cuestionario de Avalúo de Riesgos incluirá información sobre las medidas de controles establecidos para proteger los activos y sistemas de información y para mitigar los riesgos. [sic] [Apartado a.2)d)]

Véanse las recomendaciones de la 1 a la 3.

Hallazgo 2 - Falta de planes de seguridad sobre los sistemas de información del Recinto

Situación

- a. El Recinto no había preparado un plan de seguridad que incluyera los sistemas de información de la DTAA y los de las 17 áreas de servicios técnicos correspondientes a los centros de cómputos que se mantenían en las diferentes escuelas, facultades, divisiones, oficinas administrativas y decanatos. En su lugar, los planes de seguridad se prepararon individualmente para 13 áreas de servicios técnicos y

la DTAA. Para las restantes 4 áreas⁴ no se habían preparado los referidos planes de seguridad. Dichos planes deben incluir, entre otras cosas, disposiciones relacionadas con:

- La documentación de la validación de las normas de seguridad⁵
- La evidencia de un análisis de riesgos 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 para el equipo clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios, y que permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de la información (datos, programación, equipo y personal, entre otros).

Criterio

Esta situación se aparta de 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 específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la entidad, particularmente sus sistemas de misión crítica.

⁴ Véase la nota al calce 2.

⁵ 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 análisis de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

Efectos

La situación comentada 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 la Rectora no había promulgado una directriz para la preparación de un plan de seguridad integral, que abarcara todos los sistemas de información del Recinto, ni de planes individuales para cada una de las áreas de servicios técnicos.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

La persona a designarse en el rol de Seguridad de Información en la DTAA, como parte del plan 2011-2014, elaborará un plan para la revisión de las políticas de Seguridad de Información. Esta revisión incluirá documentación sobre los estándares de seguridad recomendados por la DTAA y tomará en consideración los resultados del informe de avalúo de riesgos. La política indicará las responsabilidades de la gerencia de la DTAA y demás componentes de la unidad. Se desarrollará un plan para el adiestramiento continuo (“Awareness Program”) de nuevos empleados y contratistas dentro del plan de trabajo anual 2011-2013. [sic]

Véanse las recomendaciones 1, 2 y 4.

Hallazgo 3 - Deficiencias en el Plan de Contingencia de la División de Tecnologías Académicas y Administrativas, y falta de pruebas o simulacros para comprobar su efectividad**Situaciones**

- a. El *Plan de Contingencia de la División de Tecnologías Académicas y Administrativas (Plan)*, aprobado el 18 de diciembre del 2009 por el Director Ejecutivo de la DTAA, no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:
 - Los procedimientos a seguir cuando el centro de cómputos no pueda recibir ni transmitir información

- El detalle de la configuración de los equipos críticos (equipos de comunicaciones y servidores)
 - El detalle del contenido de los respaldos, y el nombre de las librerías y de los archivos
 - El procedimiento para efectuar pruebas en el centro alterno
 - Una hoja de cotejo para verificar los daños ocasionados.
- b. Al 22 de julio de 2009, la DTAA no había efectuado procedimientos de prueba o simulacros que certificaran la efectividad del *Plan*.

Crterios

Las mejores prácticas en el campo de la tecnología de información utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte del *Plan de Continuidad de Negocios* se deberá preparar un *Plan de Contingencias*. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afectan su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la entidad, y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado a.]** Además, se deben efectuar pruebas o simulacros, por lo menos dos veces al año, revisar el *Plan* en una base trimestral y darlo a conocer a todo el personal que llevará a cabo los procesos del mismo. **[Apartado b.]**

Efectos

Las situaciones comentadas podrían 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 servicios a los usuarios del Recinto.

Causas

Las situaciones comentadas se debían a que el Director Ejecutivo de la DTAA:

- No había considerado la importancia de incluir aspectos en el *Plan* que sirvieran como herramientas para responder ante cualquier incidente, desastre o emergencia que ocurriera, y que garantizaran la continuidad de las operaciones. [Apartado a.]
- No había coordinado las pruebas y los simulacros correspondientes. [Apartado b.]

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Actualmente estamos trabajando las iniciativas de migración [...], la implementación de un ambiente virtualizado y la implementación del nuevo sistema de información estudiantil [...], como parte del plan de la DTAA del 2011-2014. Dado a los cambios en la infraestructura, interfaces entre aplicaciones y nuevas plataformas se elaborará un nuevo plan de contingencias que apoye este ambiente. [sic]

Para lograrlo, se establecerá el rol de Coordinador de Contingencias. La persona designada elaborará un plan de trabajo para el diseño de un plan de contingencias que incluya los requisitos mencionados en los incisos 4.a y 4.b. [sic]

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

Hallazgo 4 - Deficiencias en los parámetros relacionados con las políticas de auditoría de los servidores

Situaciones

- a. El examen realizado sobre los parámetros relacionados con las políticas de auditoría (*audit policies*) de cinco servidores de la red reveló las siguientes deficiencias:
 - 1) En un servidor⁶ no se habían definido las políticas de auditoría para que el sistema produjera un registro para el encendido y el

⁶ Los nombres de los servidores se incluyeron en el borrador de los hallazgos del *Informe* remitido a la Rectora y a la ex-Rectora del Recinto para comentarios.

apagado de la computadora (*restart and shutdown*), los cambios a las políticas de seguridad (*security policy changes*), y la administración de usuarios o grupos (*user group management*).

- 2) En cuatro servidores⁵ no se habían definido las políticas de auditoría para que el sistema produjera un registro para el acceso a los archivos y a los objetos (*File/object access*), el uso de los privilegios asignados a los usuarios (*use of user rights*), y el seguimiento de los procesos (*process tracking*).

Criterio

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, entre otras cosas, que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Además, se establece que los privilegios de acceso de los usuarios deberán ser reevaluados regularmente. Esta norma se instrumenta, en parte, mediante la impresión y el examen continuo de los informes que detallan los eventos inusuales del sistema.

Efectos

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

Causa

Las situaciones comentadas se debían, en parte, a que el Director Ejecutivo de la DTAA y el personal encargado de administrar los sistemas operativos en los decanatos de Administración y de Estudiantes, no habían establecido controles adecuados para la administración de las configuraciones de los servidores correspondientes a los parámetros sobre las políticas de auditoría.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

La activación de los AUDIT LOGS requiere que se realice un análisis de los eventos a guardarse en el LOG, cantidad de espacio requerido, impacto en el “performance” del servidor y tiempo de almacenaje, entre otros. Realizaremos este análisis como parte del plan de trabajo 2012-13 y luego de completadas las iniciativas de Virtualización, Active Directory y conversión de ALPHA a INTEGRITY. [sic]

Véanse las recomendaciones 1, 2, 5.c. y 6.

Hallazgo 5 - Deficiencias relacionadas con el acceso físico a los cuartos de distribución de cableado y con los estantes en los que se encontraban los equipos de comunicación

Situaciones

- a. La Secretaría Administrativa IV de la DTAA tenía la responsabilidad de mantener la custodia y el control de las llaves para acceder los cuartos de distribución de cableado. El control de las llaves se efectuaba mediante un registro donde se indicaba la hora y la fecha en que se entregaba la llave, el nombre de la persona a la que se le entregaba y el número de la misma. Si la llave se entregaba a personal externo, se anotaba el nombre de la compañía a la que este representaba. Una vez la persona entregaba la llave, se registraba la fecha y la hora en que se devolvió la misma y la firma de la persona que la entregó.

De acuerdo con lo certificado por el Director Ejecutivo de la DTAA, había seis empleados autorizados a acceder a los diferentes cuartos de distribución de cableado del Recinto. Además, una compañía tenía acceso a los mismos para atender el cuadro telefónico.

El examen efectuado sobre la información incluida en el registro durante el período del 7 de diciembre de 2009 al 10 de enero de 2010, reveló lo siguiente:

- 1) A siete personas se les hizo entrega de una llave de cuartos de distribución de cableado, a pesar de que no estaban autorizadas a acceder a los mismos.

- 2) El registro no estaba debidamente completado. Hubo ocasiones en que no se anotaron en este los apellidos de la persona a la que se le entregó la llave, la hora de la devolución de esta y la firma de la persona que devolvió la misma. Además, en el registro se anotaron nombres ilegibles.
- b. Entre el 3 y el 10 de febrero de 2010 se visitaron las áreas donde se mantenían 15 estantes con los equipos de comunicación de la red del Recinto. El examen realizado reveló las siguientes deficiencias:
- 1) En 5 estantes⁷ (33 por ciento), además del equipo de comunicación, se mantenía el equipo de telefonía.
 - 2) En cinco estantes⁷ no existía la protección adecuada para impedir que personal no autorizado pudiera tener acceso a los equipos de comunicación que se mantenían en los mismos.
 - 3) En 6 estantes⁷ (40 por ciento) los equipos de comunicación estaban expuestos a material inflamable.

Criterios

Las situaciones comentadas en los **apartados a. y b.2)** son contrarias a lo establecido en Sección 3.1 de la *Política y Procedimiento de Mantenimiento de la Infraestructura Tecnológica*, aprobada el 31 de marzo de 2009 por el Director Ejecutivo de la DTAA.

Las mejores prácticas en el campo de la tecnología de información sugieren que las entidades deberán tomar los cuidados necesarios para proteger y mantener en óptimas condiciones los equipos computadorizados, y evitar daños y averías. El propósito es asegurar la integridad, la exactitud y la disponibilidad de la información, y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y de los sistemas computadorizados, es necesario que se mantengan los equipos de

⁷ La localización de los estantes se incluyó en el borrador de los **hallazgos** del *Informe* remitido a la Rectora y a la ex-Rectora del Recinto para comentarios.

computadoras y de comunicaciones en un lugar seguro, que provea las condiciones ambientales y físicas adecuadas, y que se controle adecuadamente el acceso a los mismos. [Apartados a. y b.]

Efectos

Las situaciones comentadas en los **apartados a., y b.1) y 2)** facilitan que personas ajenas a las operaciones tengan acceso a los equipos de comunicación, y que puedan hacer uso indebido de este, manipular o destruir datos o causar daños físicos a la propiedad. Esto representa un riesgo para la continuidad de los servicios que ofrece el Recinto, así como para la confidencialidad de la información que se procesa.

La situación comentada en el **apartado b.3)** pudiera ocasionar daños y deterioros prematuros a los equipos de la red, lo que podría impedir obtener el rendimiento máximo en términos de los servicios que estos ofrecen.

Causas

La situación comentada en el **apartado a.1)** se debía a que el Director Ejecutivo de la DTAA no le había informado a la persona encargada de la custodia y del control de las llaves de los cuartos de distribución de cableado, los nombres de las personas que estaban autorizadas a acceder a los mismos.

La situación comentada en el **apartado a.2)** se debió a la falta de una supervisión efectiva por parte del Director Ejecutivo de la DTAA, para asegurarse de que el registro se completara adecuadamente.

Las situaciones comentadas en el **apartado b.** se debían a que el Director Ejecutivo de la DTAA no había cumplido con su deber de velar por que los cuartos de distribución de cableado estuvieran ubicados en lugares adecuados y seguros, a los que solo pudiera acceder el personal autorizado, y en los que los equipos no estuvieran expuestos a daños ambientales.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Para este hallazgo fue corregido mediante la modificación del formulario de "Registro del uso de las llaves de los cuartos de

telecomunicaciones del Recinto". En este documento se integraron los nombres de las personas autorizadas a tomar prestada la llave. Además, se especificó que deberán llenar todos los campos requeridos del documento y en forma legible. También se designa responsabilidad en la secretaria del área, la cual fue debidamente orientada, para la verificación del cumplimiento de estas directrices e informar sobre cualquier irregularidad. [sic] [Apartado a.]

Aunque en algunos cuartos de comunicaciones también se mantiene almacenado algún equipo de telefonía, el acceso al área esta restringido al personal designado de la DTAA y al personal que provee mantenimiento a los equipos. El riesgo de exposición de estos equipos es mínimo. [sic] [Apartado b.1)]

Los estantes con equipo de comunicación ubicados en [...] fueron ubicados en cuartos de comunicaciones controlados por llave. [Apartado b.2)]

Se removió el material inflamable que estaba ubicado en los cuartos de comunicaciones. [Apartado b.3)]

Véanse las recomendaciones 1, 2 y 5 de la d. a la g.

Hallazgo 6 - Deficiencias relacionadas con el almacenamiento de los respaldos de los archivos computadorizados de información

Situación

- a. Al 17 de marzo de 2010, la DTAA poseía dos métodos para hacer respaldos de los archivos computadorizados de información. El primero estaba integrado a los servidores *Alpha*, en los cuales se procesaban las transacciones de las aplicaciones administrativas principales del Recinto, tales como el Sistema de Información Estudiantil (SIS), el Sistema de Recursos Humanos (HRS) y el Sistema de Propiedad. En el segundo método los respaldos se preparaban a través de una aplicación conocida como *Networker* (previamente llamada *Legato*). Mediante esta se producían los respaldos de los servidores que la DTAA administraba, entre los que se incluían servidores de otras escuelas, decanatos y facultades, los cuales estaban localizados dentro del centro de cómputos de la

DTAA (*Server Farm*)⁸. Este método de respaldo también almacenaba toda la información proveniente de los servidores *Alpha*. El examen realizado a estos respaldos reveló las siguientes deficiencias:

- 1) Los respaldos realizados a los servidores *Alpha* no se mantenían en un lugar seguro fuera de los predios del Recinto.
- 2) Los respaldos realizados con la aplicación *Networker* no se mantenían por un período mayor a dos semanas.

Crterios

Las situaciones comentadas son contrarias a lo establecido en el Título 5.5, *Período de Retención, Vida Útil y Disposición de Medios Magnéticos*, de las *Normas y Procedimientos de Resguardos*, aprobadas el 27 de octubre de 2009 por el Director Ejecutivo de la DTAA. Además, son contrarias a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

Efecto

Las situaciones comentadas pueden ocasionar que, en casos de emergencias, el Recinto no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Causa

Las situaciones comentadas se debían, en parte, a que el Director Ejecutivo de la DTAA no tomó las debidas precauciones para asegurarse de que los empleados encargados de realizar los respaldos cumplieran con lo establecido en las *Normas y Procedimientos de Resguardos* y en la *Carta Circular Núm. 77-05*.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

En marzo de 2011 se modificaron los procedimientos existentes en el documento de "Normas y Procedimientos de Resguardos". [sic]

Véanse las recomendaciones 1, 2 y 5.h.

⁸ Grupo de computadoras utilizadas como servidores que, por lo regular, pueden representar docenas o cientos de estas, y que son mantenidas todas en un mismo lugar. Al *Server Farm* también se le conoce como *Server Cluster*.

Hallazgo 7 - Procedimientos sin aprobar por la Rectora del Recinto**Situación**

a. Al 4 de diciembre de 2009, los siguientes procedimientos y normas relacionados con los sistemas de información computadorizados no estaban aprobados por la Rectora del Recinto:

- *Procedimiento Sobre Pruebas e Implantación de Programas*
- *Normas de Documentación*
- *Normas y Procedimientos para la Conexión de Equipos detrás del Firewall*
- *Normas y Procedimientos de Mantenimiento de la Infraestructura Tecnológica*
- *Normas y Procedimientos para la Eliminación de Datos en Equipos de Computación*
- *Normas y Procedimientos de Cuentas de Usuarios*
- *Normas y Procedimientos de Resguardos*
- *Normas para el Manejo de Cuentas con Privilegios de Administrador.*

Criterio

Esta situación es contraria 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 específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica.

Efecto

La situación comentada podría ocasionar que las operaciones de los sistemas de información del Recinto no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias.

Causa

La situación comentada se debió a que el Director Ejecutivo de la DTAA no había remitido para la aprobación de la Rectora las normas y los procedimientos mencionados.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Se estarán actualizando las políticas y procedimientos de la DTAA como parte del plan de trabajo 2011-2014 para alinearlos con los cambios en la infraestructura, nuevas tecnologías, herramientas y procesos. Luego de completados los cambios se someterán a la Oficina de Normas y Auditoría para revisión de estándares y referido a la Rectora para su aprobación. Se orientará a la gerencia sobre el protocolo a seguir para la publicación de políticas en el Recinto el cual requiere la aprobación de la Rectora. [sic]

Véanse las recomendaciones 1, 2 y 5.i.

Hallazgo 8 - Falta de controles adecuados de los formularios de cheques en blanco, y de los discos compactos que contiene las firmas autorizadas para pago**Situaciones**

- a. Los cheques para el pago de la nómina de los empleados, de los proveedores de servicios y de los reembolsos a estudiantes del Recinto, se imprimían en el Centro de Cómputos de la DTAA. Para la impresión de los cheques, se utilizaban formularios de cheques en blanco que incluían preimpresos el número de cheque al frente y un número de control secuencial por la parte de atrás. Para firmar los cheques, se utilizaban discos compactos, que contenían las firmas autorizadas para el pago de los mismos.

El examen efectuado el 5 de noviembre de 2009 sobre los controles relacionados con los formularios y los discos compactos con las firmas autorizadas para pago, reveló que los mismos no se mantenían bajo la custodia de un área ajena a la que estaba a cargo de imprimir los cheques, según se indica:

- 1) En el almacén de las cintas de respaldos, localizado dentro de las instalaciones de la DTAA, identificamos dos cajas de

formularios de cheques en blanco sin abrir y una abierta. La caja que estaba abierta tenía un papel que identificaba la numeración del último cheque que fue impreso. A este almacén tenían acceso cuatro Operadores de Computador Electrónico II de la DTAA.

- 2) Los discos compactos con las firmas autorizadas estaban dentro de un anaquel de madera con llave en el almacén de cintas de respaldos dentro de las instalaciones de la DTAA. De esta llave tenían copia el Director de la DTAA, el Supervisor de Operaciones Computadorizadas de la DTAA y el personal de Pagaduría de la Oficina de Finanzas. La copia de la llave que tenía el Supervisor de Operaciones Computadorizadas de la DTAA también era utilizada por cuatro Operadores de Computador Electrónico II.

Criterio

Es norma de sana administración que los cheques en blanco y los discos compactos que contienen las firmas autorizadas para pago estén bajo la custodia de áreas ajenas a la que imprime los mismos.

Efecto

Las situaciones comentadas pueden propiciar el uso indebido de los cheques en blanco sin que se pueda detectar a tiempo para fijar responsabilidades.

Causa

Las situaciones comentadas se debían a que la Rectora no había impartido instrucciones para que el Decano de Administración se asegurara de que la custodia de los cheques en blanco y de los discos compactos con las firmas autorizadas para pagos, estuviera bajo un área ajena a la DTAA, quien estaba a cargo de imprimir los cheques.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Se procedió a colocar las cajas con los formularios de cheques en blanco en el área de almacenaje de cartuchos. Esta unidad tiene control de acceso y solamente la acceden los operadores del Data

Center. El CD con las firmas autorizadas está guardado bajo llave en [...]. Se presentará un plan para la transferencia de este proceso a Finanzas dentro del plan de trabajo anual 2011-2013. [sic]

Véanse las recomendaciones 1, 2 y 7.a.

Hallazgo 9 - Falta de documentación relacionada con la justificación y la autorización de los accesos a las cuentas con privilegios de administrador, y del otorgamiento de privilegios de conexión remota a los sistemas de información

Situación

- a. Al 17 de septiembre de 2009, el Director Ejecutivo de la DTAA no pudo proveer a nuestros auditores la documentación relacionada con:
 - 1) La justificación y la autorización para otorgar cuentas de accesos con privilegios de administrador a los sistemas. Una cuenta como esta tiene amplios privilegios que permiten, entre otras cosas, realizar cambios a la configuración del sistema, instalar programas y equipos, acceder a todos los archivos de la computadora, y realizar cambios a las cuentas de otros usuarios.
 - 2) El otorgamiento del privilegio de conexión remota para las 17 cuentas de acceso remoto existentes. Este tipo de privilegio permite acceder y utilizar la información computadorizada de una entidad desde un lugar remoto o distinto de donde está guardada la misma.

Criterios

Las situaciones comentadas se apartan de lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establece que:

- La información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos necesarios, o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deberán incluir mecanismos de autenticación y autorización. **[Apartado a.1)]**
- Si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para

que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. [Apartado a.2)]

Efecto

Las situaciones comentadas impiden mantener la evidencia requerida para determinar si las cuentas de acceso con los privilegios de administrador de los sistemas y las cuentas de acceso remoto, están debidamente autorizadas y si estas son asignadas conforme a las funciones y a los deberes de los usuarios que utilizan las mismas.

Causa

Las situaciones comentadas se debieron a que el Director Ejecutivo de la DTAA entendía que no era necesario documentar la justificación de las cuentas de acceso con privilegios de administrador de sistemas y de acceso remoto debido a que dichos accesos fueron otorgados a personal cuyas funciones lo requieren.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Dentro de las iniciativas de integración de los dominios de Active Directory a un Directorio Unificado realizaremos una revisión del personal con privilegios de administrador. Esta revisión incluye al personal de la DTAA y al personal técnico destacado en las Facultades. Se revalidarán los accesos y se documentará todo el proceso. Además, como parte del plan de trabajo 2011-2014 se realizará una revisión del personal con acceso remoto a la red y se documentaran los casos. [sic]

Véanse las recomendaciones 1, 2, 5.j. y 7.b.

Hallazgo 10 - Falta de revisiones periódicas de los registros de auditoría producidos por el sistema y de los accesos a Internet

Situaciones

- a. Al 23 de noviembre de 2009, el Director de Servicios Técnicos en Tecnología de Información de la DTAA no examinaba periódicamente los registros de auditoría (*logs*) del sistema para

conocer los posibles problemas que podían ocurrir en los servidores o en la red de comunicación, y tomar las medidas preventivas y correctivas prontamente.

- b. Al 15 de abril de 2010, el personal de la DTAA encargado de la seguridad de los sistemas no verificaba los accesos a Internet por parte de los usuarios conectados a la red del Recinto.

Criterio

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*, relacionado con la revisión de las actividades de los usuarios en los activos críticos.

Efectos

Las situaciones comentadas impiden la detección temprana de:

- Errores críticos o problemas con el sistema que permitan tomar de inmediato las medidas preventivas y correctivas necesarias.

[Apartado a.]

- Actividades o usos de Internet no autorizados que permitan a la gerencia tomar medidas preventivas y correctivas a tiempo.

[Apartado b.]

Causas

La situación comentada en el **apartado a.** se debía a que el Director de Servicios Técnicos en Tecnología de Información solo revisaba dichos registros cuando surgían anomalías en algún proceso.

La situación comentada en el **apartado b.** se debía a que existía una gran cantidad de cuentas que tenían acceso a Internet, por lo que al personal que trabajaba en la DTAA se le hacía difícil la revisión de los accesos de estas.

Comentarios de la Gerencia

En la carta de la Rectora, esta nos indicó, entre otras cosas, lo siguiente:

Como parte de las iniciativas del proyecto [...] se implementarán varias herramientas [...] para la administración de la red. Estas herramientas serán implementadas durante el plan de 2011-2014. La herramienta [...] le proveerá al personal de Operaciones las

herramientas necesarias para el monitoreo de los servidores. El monitoreo sobre la utilización del Internet requiere ser evaluado y la adquisición de una herramienta que ayude a filtrar los eventos. [sic]

Véanse las recomendaciones 1, 2, y 5.k. y l.

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 10]

Al Presidente de la Universidad de Puerto Rico

2. Ver que la Rectora del Recinto cumpla con las **recomendaciones de la 3 a la 7** de este *Informe*. [Hallazgos del 1 al 10]

A la Rectora del Recinto de Río Piedras

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 seguridad que integre todos los sistemas de información del Recinto, y que incluya los criterios descritos en el **Hallazgo 2**, o de que las áreas de servicios técnicos que no cuentan con estos planes preparen y documenten los mismos. 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.
5. Ejercer una supervisión efectiva sobre la Directora Ejecutiva de la DTAA para asegurarse de que:
 - a. Se revise el *Plan* para que incluya los aspectos comentados en el **Hallazgo 3-a**.
 - b. Se realicen procedimientos de pruebas y simulacros, y se documenten los resultados de estos. [Hallazgo 3-b.]

- c. Se activen las opciones correspondientes en la pantalla de políticas de auditorías (*Audit Policies*) que se mencionan en el **Hallazgo 4**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la DTAA.
- d. Se provea a la persona encargada de la custodia y del control de las llaves de los cuartos de distribución de cableado, una lista de las personas autorizadas a acceder a los mismos. **[Hallazgo 5-a.1)]**
- e. La persona encargada de la custodia y del control de las llaves de los cuartos de distribución de cableado, se asegure de que el registro, mediante el cual se mantiene este control, sea completado en su totalidad y que la información incluida en el mismo sea legible. **[Hallazgo 5-a.2)]**
- f. Se establezcan las medidas necesarias para la protección física de los equipos de comunicación de la red del Recinto, de manera que no estén accesibles a personal ajeno a las operaciones de este. **[Hallazgo 5-b.1) y 2)]**
- g. Se establezcan las medidas necesarias para mantener controles ambientales adecuados en los cuartos de distribución de cableado, de manera que los equipos de comunicación de la red del Recinto no estén expuestos daños y deterioros prematuros, que puedan impedir el obtener su máximo rendimiento. **[Hallazgo 5-b.3)]**
- h. Los empleados encargados de hacer los respaldos de la información cumplan con lo establecido en el procedimiento *Normas y Procedimientos de Resguardos* y en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. **[Hallazgo 6]**
- i. Revise y remita para su consideración y aprobación, las normas y los procedimientos escritos necesarios para regir las operaciones de la DTAA que se comentan en el **Hallazgo 7**.

- j. Los accesos con privilegios de administrador de los sistemas y de conexión remota estén debidamente justificados, autorizados y documentados. **[Hallazgo 9]**
 - k. El Director de Servicios Técnicos en Tecnología de Información revise periódicamente, como parte de las operaciones regulares de la DTAA, los registros de acceso que producen los servidores principales de la red de comunicaciones, y documente la revisión de los mismos. **[Hallazgo 10-a.]**
 - l. Se identifiquen herramientas tecnológicas para el control de los accesos a Internet, que contribuyan en la revisión de estos, y que permitan detectar a tiempo actividades o usos no autorizados, para tomar medidas preventivas y correctivas. **[Hallazgo 10-b.]**
6. Ejercer una supervisión efectiva sobre los decanos de Administración y de Estudiantes para asegurarse de que el personal encargado de administrar los servidores de sus correspondientes decanatos, activen las opciones en la pantalla de políticas de auditoría (*Audit policies*) que se mencionan en el **Hallazgo 4**. Esto, de manera que se pueda mantener un rastro de las actividades realizadas en dichos servidores.
7. Ejercer una supervisión efectiva sobre el Decano de Administración para asegurarse de que:
- a. Un área ajena a la que está a cargo de imprimir los cheques mantenga la custodia y el control de los formularios de cheques en blanco, y de los discos compactos con las firmas autorizadas. **[Hallazgo 8]**
 - b. Las cuentas del Decanato con privilegios de conexión remota estén debidamente justificadas, autorizadas y documentadas. **[Hallazgo 9-a.2)]**

AGRADECIMIENTO

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

Comisaria del Central
Por: *Fernán M. Valderrama*

ANEJO 1

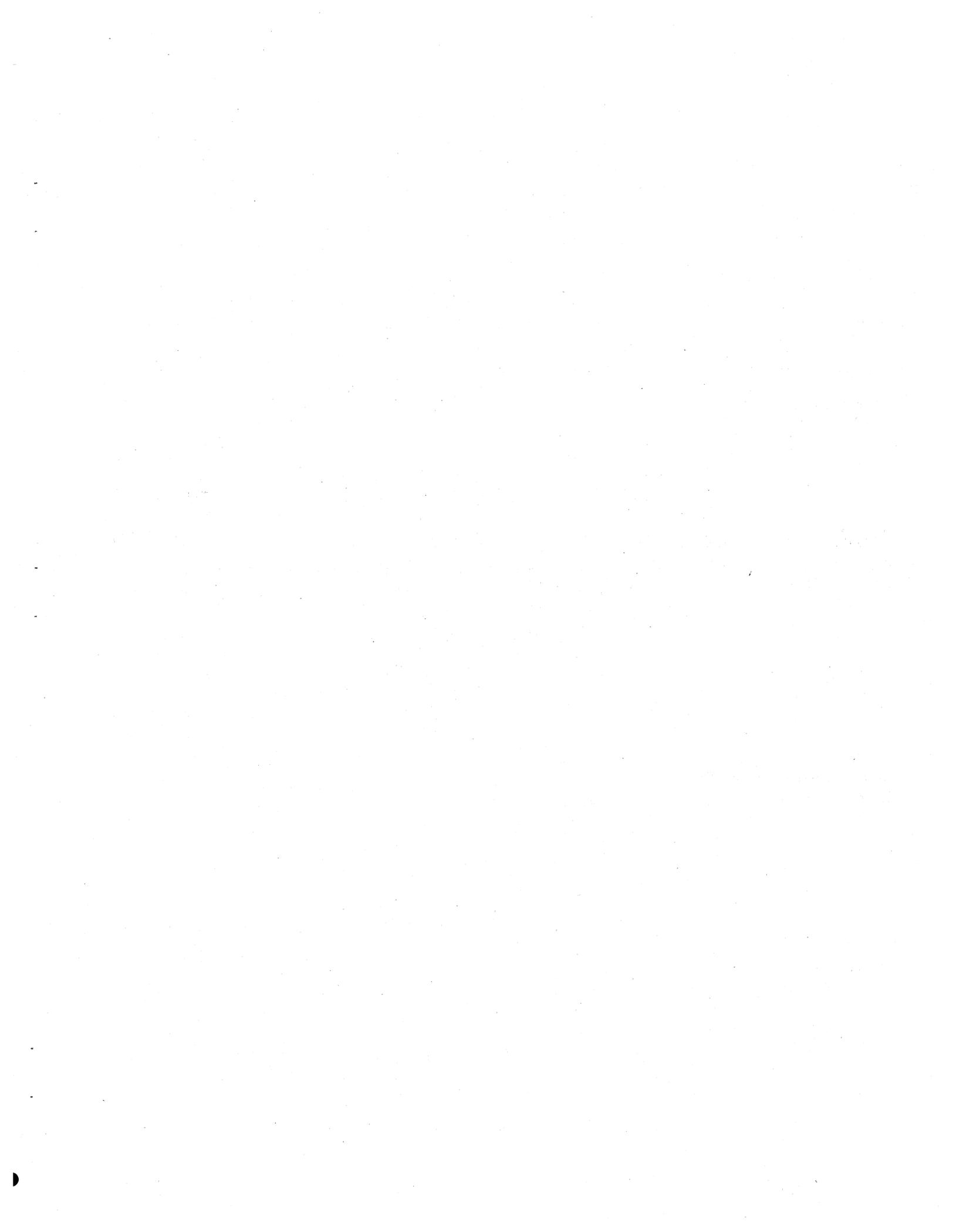
UNIVERSIDAD DE PUERTO RICO
RECINTO DE RÍO PIEDRAS
DIVISIÓN DE TECNOLOGÍAS ACADÉMICAS Y ADMINISTRATIVAS
**MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Ygrí Rivera de Martínez	Presidenta	28 jun. 09	17 m. 10
Ing. Carlos H. del Río Rodríguez	Presidente	22 m. 09	27 jun. 09
CPA Carlos J. Dávila Torres	Vicepresidente	28 jun. 09	17 m. 10
Ing. Carlos I. Pesquera Morales	"	22 m. 09	27 jun. 09
Dra. Rosa A. Franqui Rivera	Secretaria	22 oct. 09	17 m. 10
Lcdo. Salvador Antonetti Zequeira	Secretario	22 m. 09	4 oct. 09

ANEJO 2

UNIVERSIDAD DE PUERTO RICO
 RECINTO DE RÍO PIEDRAS
 DIVISIÓN DE TECNOLOGÍAS ACADÉMICAS Y ADMINISTRATIVAS
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
 DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dra. Ana R. Guadalupe Quiñones	Rectora	1 oct. 09	17 m. 10
Dra. Gladys Escalona De Motta	"	22 m. 09	30 sep. 09
Sr. José J. Estrada Peña	Decano de Administración	22 m. 09	17 m. 10
Dra. Mayra Charriez	Decana de Estudiantes Interina	14 dic. 09	17 m. 10
Dra. Ivonne F. Moreno Velázquez	"	22 m. 09	11 dic. 09
Ing. Denisse Figueroa Irizarry	Directora Ejecutiva de la DTAA	1 abr. 10	17 m. 10
Dr. Edwin J. Martínez Hernández	Director Ejecutivo de la DTAA	22 m. 09	31 mar. 10
Sr. Alberto Feliciano Nieves	Director de Recursos Humanos	22 m. 09	17 m. 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

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

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

Correo electrónico:

ocpr@ocpr.gov.pr