17/sept/2012

SENADO
GOBIERNO DE PUERTO RICO

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 Eonómico 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 Ricc
- ☐ Sobre Reforma Gubernamental

COMISIONES CONJUNTAS

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

Iniciales

SENADO
GOBIERNO DE PUERTO RICO

Oficina del Presidente

Katherine Erazo
CHIEF OF STAFF

Fecha 14 de septiembre 2012

Referido a Brunilda Ortiz

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

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ
2012 SEP 13 AM 11:24

13 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 copia del *Informe de Auditoría TI-13-04* de la Oficina de Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico, aprobado por esta Oficina el 8 de septiembre 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

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

2-191083

[redacted]

INFORME DE AUDITORÍA TI-13-04

8 de septiembre de 2012

Compañía de Parques Nacionales de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5212 - Auditoría 13308)

Período auditado: 19 de junio de 2009 al 5 de marzo de 2010

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ

2012 SEP 13 AM 11:24

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **5**

OPINIÓN Y HALLAZGOS **6**

1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados 6

2 - Falta de un plan de seguridad y de acuerdos de confidencialidad 8

3 - Falta de un plan de continuidad de negocios, deficiencias en el Plan de Contingencias, falta de pruebas o simulacros que certificaran la efectividad del Plan, y falta de un centro alterno para la recuperación de las operaciones computadorizadas 10

4 - Deficiencias relacionadas con la información del equipo y de los programas mantenida en el Módulo de Inventario del Sistema Oracle Financials, y falta de un registro de los programas instalados en las computadoras 14

5 - Deficiencias relacionadas con la producción y el almacenamiento de los respaldos de los archivos computadorizados de información 18

6 - Deficiencias relacionadas con los parámetros de control de acceso, y mantenimiento inadecuado de las cuentas de acceso 20

7 - Falta de un formulario para solicitar la modificación de los privilegios de las cuentas de acceso 21

8 - Falta de normas y de procedimientos escritos para la administración y la seguridad de los sistemas computadorizados; de documentación sobre la entrega del Manual de Acceso; y de adiestramientos y pantallas de advertencias para concienciar sobre las normas establecidas para el uso y el control de los equipos y de los sistemas computadorizados 23

9 - Falta de revisiones periódicas de los registros de eventos de los sistemas operativos y de los incidentes de seguridad de la red 28

RECOMENDACIONES **29**

AGRADECIMIENTO **33**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **34**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **35**

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

8 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 Oficina de Sistemas de Información (OSI) de la Compañía de Parques Nacionales de Puerto Rico (Compañía) 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 19 de junio de 2009 al 5 de marzo de 2010. En algunos aspectos examinamos operaciones 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, pruebas y análisis de procedimientos de control interno y de otros procesos, y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este es el primer informe, y contiene nueve hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, la continuidad del servicio, el acceso lógico y físico, y la red de comunicaciones de la Compañía.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Compañía fue creada mediante la *Ley 10-2001* que enmendó la *Ley Núm. 114 del 23 de junio de 1961, Ley de la Compañía de Parques Nacionales de Puerto Rico*, según enmendada. Por medio de la *Ley 10-2001*, se integró el Fideicomiso para el Desarrollo, Operación y Conservación de los Parques Nacionales de Puerto Rico, creado mediante la Escritura Núm. 3 otorgada ante notario público el 23 de diciembre de 1988, con la Compañía de Fomento Recreativo de Puerto Rico, creada mediante la *Ley Núm. 114*. En la *Ley 10-2001* se dispuso que la Compañía operará un sistema que integre todos los parques naturales, recreativos e históricos que sean declarados como nacionales. También promoverá la protección, la conservación y el uso recreativo de parques, playas, bosques, monumentos históricos y naturales de Puerto Rico, de tal forma que se preserven y se mantengan en óptimo estado para el disfrute de las presentes y futuras generaciones de puertorriqueños y visitantes del exterior.

Los poderes y la política pública de la Compañía son ejercidos por una Junta de Directores (Junta) compuesta por 9 miembros. El Secretario de Recreación y Deportes es el Presidente de la Junta. Además, 3 de los miembros son el Secretario de Educación, el Director Ejecutivo de la Compañía de Turismo de Puerto Rico y el Secretario de Recursos Naturales y Ambientales, o cualquier funcionario designado por estos. Los restantes 5 miembros serán personas de reconocido interés y trayectoria en el desarrollo y la preservación de los parques en el sector privado, y serán nombrados por el Gobernador con la recomendación del Presidente de la Junta. El Gobernador podrá sustituir estos 5 miembros cuando lo entienda apropiado y necesario para lograr los objetivos de la *Ley 10-2001*. En caso de ocurrir una vacante, esta se cubrirá dentro de los 60 días siguientes.

El Director Ejecutivo de la Compañía es nombrado por el Gobernador con la recomendación del Presidente de la Junta. El Director Ejecutivo, entre otras funciones, administra las operaciones de la Compañía y le responde

a la Junta. Esta podrá delegar en el Director Ejecutivo cualquiera de sus poderes, excepto el adoptar normas y reglamentos, y el aprobar el presupuesto de la Compañía.

A la fecha de nuestra auditoría, la Compañía realizaba sus operaciones a través de las siguientes unidades que respondían al Director Ejecutivo: la Oficina de Asesoramiento Legal, la Oficina de Comunicaciones y Prensa, la Oficina de Administración, la Oficina de Recursos Humanos, la Oficina de Presupuesto y Finanzas, la Oficina de Mercadeo y Servicios al Cliente, la Oficina de Planificación, Recursos Externos y Mejoras Permanentes, la División de Operaciones de Parques, el Parque Las Cavernas del Río Camuy, el Parque del Zoológico Dr. Juan A. Rivero y la OSI. Además, la Compañía contaba con una Oficina de Auditoría Interna que le respondía directamente a la Junta.

La OSI contaba con una Ayudante Especial que fungía como Directora de Sistemas de Información, un Director Auxiliar de Sistemas de Información, un Oficial de Redes de Comunicación, un Desarrollador de Sistemas de Informática, un Operador de la Unidad Central de Informática y un Especialista en Recursos Humanos. Este último fue autorizado a laborar en la OSI mediante un traslado administrativo.

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

La Compañía administraba cinco centros vacacionales: el Centro Vacacional de Boquerón, el Centro Vacacional Monte del Estado, el Centro Vacacional Punta Guilarte, el Centro Vacacional Punta Santiago y las Villas de Añasco. Además, administraba las instalaciones ubicadas en los balnearios de Boquerón, Caña Gorda, Cerro Gordo, La Monserrate, Manuel Nolo Morales, Playita, Punta Guilarte, Punta Salinas, Punta Santiago, Seven Seas, Sun Bay y Tres Hermanos. También administraba los siguientes parques y áreas recreativas: el Área Recreativa de Isla de Cabras, las casas de remolque en los balnearios de Punta Guilarte, Punta Santiago y Seven Seas, el Parque del Zoológico Dr. Juan A. Rivero,

el Parque Acuático Infantil, el Parque Julio Enrique Monagas, el Parque en la Laguna del Condado, el Parque Luis Muñoz Marín, el Parque Luis Muñoz Rivera, el Parque Nacional Río Tanamá en Utuado y el Parque del Tercer Milenio José Celso Barbosa.

Los recursos para financiar las actividades operacionales de la Compañía provienen primordialmente de asignaciones legislativas e ingresos propios por el arrendamiento de casetas, villas y cabañas; por la venta de boletos de entrada a las instalaciones y a las atracciones; por los concesionarios; y por las actividades especiales. El presupuesto de la Compañía para los años del 2007-08 al 2009-10 ascendió a $36,868,000, $37,272,377 y $29,544,000, respectivamente. Durante los años fiscales 2007-08 y 2008-09 fueron asignados a la OSI $296,476 y $347,075, respectivamente[1].

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

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Hon. Daniel J. Galán Kercadó, Director Ejecutivo de la Compañía, mediante carta de nuestros auditores, del 9 de marzo de 2010. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

El 26 de marzo de 2010, la Sra. Felicita Pizarro Calderón, Directora de Finanzas y Presupuesto, a nombre del 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 31 de enero de 2012.

---

[1] El presupuesto de la OSI para el año fiscal 2009-10 no estuvo disponible durante la auditoría.

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* y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OSI, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, la continuidad del servicio, el acceso lógico y físico, y la red de comunicaciones de la Compañía, se realizaron sustancialmente de acuerdo con la ley y la reglamentación aplicables, excepto por los **hallazgos del 1 al 9** que se comentan a continuación.

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

Situación

a. Un análisis de riesgos de los sistemas de información computadorizados es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, 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.

Al 4 de agosto de 2009, en la Compañía no se había realizado un análisis 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 (OGP).

Efectos

La situación comentada impide a la Compañía estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y de 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 de la Compañía, en caso de que surja alguna eventualidad. **[Véase el Hallazgo 3-a.]**

Causa

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

Comentarios de la Gerencia

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

> [...] se sometió a la Junta de Directores las "**Normas sobre la realización de la Evaluación de Riesgo de la Compañía de Parques Nacionales de Puerto Rico**". [...] El 8 de agosto de 2011, el Director Ejecutivo designó el Comité de Evaluación de

> Riesgo [...]. El Comité [...] comenzó a desarrollar su Plan de Trabajo donde se propone evaluar los riesgos en todas las áreas, incluyendo la Oficina de Sistemas de Información. [*sic*]

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un plan de seguridad y de acuerdos de confidencialidad

Situaciones

a. Al 4 de agosto de 2009, la Compañía no tenía un plan de seguridad aprobado por la Junta de Directores que incluyera, entre otras cosas, disposiciones en cuanto a:

- La documentación de la validación de las normas de seguridad[2]
- La evidencia de un análisis de riesgos actualizado, que sea base del plan
- La responsabilidad de la gerencia y de los demás componentes de la unidad; tales como: los dueños y los usuarios de los recursos de información y el personal de la OSI, entre otros
- Un programa de adiestramiento especializado al personal clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios que 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)
- La documentación de la interconexión de los sistemas.

b. Al 1 de octubre de 2009, en los expedientes de la OSI no se mantenía el *Acuerdo de Confidencialidad, Seguridad de Información y Protección de Equipos* (*Acuerdo*), que debía firmar cada usuario de

---

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

los sistemas de información antes de ser expuesto a información confidencial u otros activos sensitivos. Además, en la Oficina de Recurso Humanos se mantenía el *Acuerdo* de solo dos empleados de la Compañía.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. **[Apartados a. y b.]** También se establece que las entidades gubernamentales son responsables de, entre otras cosas, establecer controles en el reclutamiento del personal de sistemas de información, especialmente para el área de seguridad, que requieran que este personal firme acuerdos de no divulgación antes de exponerlo a información confidencial u otros activos sensitivos como los programas y el equipo. **[Apartado b.]**

Además, la situación comentada en el **apartado b.** es contraria a lo establecido en el Artículo 7, Sección 7.1 de la *Política para la Administración y Manejo de los Sistemas de Información*, del *Manual de Acceso y Uso de los Sistemas de Información de la Compañía de Parques Nacionales* (*Manual de Acceso*), aprobado el 10 de octubre de 2007 por la Junta de Directores de la Compañía.

Efectos

La situación comentada en el **apartado a.** 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.

La situación comentada en el **apartado b.** dificulta fijar responsabilidad a los empleados que trabajan con información confidencial cuando la misma

es divulgada. Además, da lugar al uso indebido de la información privilegiada, lo que resultaría en otras consecuencias adversas para la Compañía.

Causas

La situación comentada en el **apartado a.** se atribuye a que el Director Ejecutivo no había impartido las directrices para que la Ayudante Especial preparara un plan de seguridad basado en un análisis de riesgos de los sistemas de información y para la implantación y la actualización continua del mismo, según lo establecido en la *Carta Circular Núm. 77-05*.

La situación comentada en el **apartado b.** se debía a que la Directora de Recursos Humanos no se aseguró de proveer a los empleados el *Acuerdo* y de cumplir con las directrices para el trámite y el manejo de este, según establecidas en el *Manual de Acceso*.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> Una vez se realice la Evaluación de Riesgo, la OSI desarrollará el Plan de Seguridad para someterlo a la Junta de Directores. [...] [*sic*] **[Apartado a.]**
>
> El *Acuerdo de confidencialidad, seguridad de información y protección de equipos* fue incluido como parte de la forma RH-2010-02 OSI 7.3 **Acuerdo de Confidencialidad y Solicitud de Cuentas para Usuarios y Correo Electrónico**. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1, 3.a. y 4.a.

Hallazgo 3 - Falta de un plan de continuidad de negocios, deficiencias en el Plan de Contingencias, falta de pruebas o simulacros que certificaran la efectividad del Plan, y falta de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Al 4 de agosto de 2009, la Compañía carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la OSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información

computadorizados y restaurar las operaciones de la OSI en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

b. El *Plan de Contingencia para los Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico* (*Plan*), aprobado el 9 de abril de 2008 por la Junta de Directores de la Compañía, no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

- La identificación de los integrantes de los grupos de recuperación y la responsabilidad asignada a cada uno de estos
- Los procedimientos a seguir cuando el centro de cómputos no puede recibir o transmitir información de los usuarios que acceden mediante conexiones remotas los sistemas de información de la Compañía
- El inventario actualizado de los equipos, de los sistemas operativos y de las aplicaciones
- La identificación de los archivos críticos de la OSI
- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar
- El detalle de la configuración de los equipos críticos (equipos de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
- El nombre del encargado de activar el *Plan* y del personal de reserva, de forma que pueda ser activado sin depender de individuos específicos
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia
- Una lista de los números de teléfonos de los miembros de cada grupo de recuperación
- Una lista del personal que recibió la copia del *Plan*

- Una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con la entidad.

c. Al 27 de agosto de 2009, la OSI no había efectuado procedimientos de prueba o simulacros que certificaran la efectividad del *Plan*.

d. Al 4 de agosto de 2009, la Compañía no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en caso de emergencia. Tampoco había formalizado acuerdos escritos con otra entidad para establecer un centro alterno en las instalaciones de esta.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en las políticas núms. *TIG-003* y *TIG-004, Servicios de Tecnología*, de la *Carta Circular Núm. 77-05*.

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 b.]** Además, se deben efectuar pruebas o simulacros por lo menos una vez al año para comprobar la efectividad de los planes. **[Apartado c.]**

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 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 d.]**

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración
- Un centro alterno de la propia entidad.

Efectos

Las situaciones comentadas en los **apartados del a. al c.** 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 y de interrupciones prolongadas de los servicios a los usuarios de la Compañía.

La situación comentada en el **apartado d.** podría afectar las funciones de la Compañía 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.

Causas

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a la falta de un análisis de riesgos de los sistemas de información computadorizados de la Compañía que sirviera de base para la preparación y la revisión del plan de continuidad de negocios. **[Hallazgo 1]**

La situación comentada en el **apartado c.** se debía a que el Director Ejecutivo no le requirió a la Ayudante Especial que efectuara las pruebas al plan diseñado por el Director Auxiliar de Sistemas de Información, para asegurarse de que este era funcional y consideraba las necesidades y los riesgos de la Compañía.

La situación comentada en el **apartado d.** se atribuye a que la Ayudante Especial no había coordinado con el Director Ejecutivo la identificación de un lugar disponible y adecuado como centro alterno para restaurar las operaciones críticas computadorizadas de la OSI.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> La OSI se encuentra en un proceso de investigación para poder redactar un plan de continuidad de negocios que vaya de acuerdo con las necesidades de la CPNPR. [...] **[Apartado a.]**
>
> El Plan de Contingencia para los Sistemas de Información de la CPNPR es uno ambiguo, ya que carece de datos esenciales para que el mismo pueda ser funcional. [...] **[Apartado b.]**
>
> En la actualidad no se han realizados simulacros que validen el procedimiento según el plan. [*sic*] **[Apartado c.]**
>
> Al 10 de febrero de 2012 estos acuerdos no existen. Se contempla mejorar el Plan de Contingencia para que este sea uno efectivo. La OSI se encuentra en búsqueda de un centro de cómputos [...] [*sic*] **[Apartado d.]**

Véanse las recomendaciones 1, 3.b. y c., 5 y 6.

Hallazgo 4 - Deficiencias relacionadas con la información del equipo y de los programas mantenida en el Módulo de Inventario del Sistema Oracle Financials, y falta de un registro de los programas instalados en las computadoras

Situaciones

a. El personal de la Oficina de Propiedad utilizaba el Módulo de Inventario del Sistema *Oracle Financials* (Módulo de Inventario) para mantener un registro de la propiedad de la Compañía, los números de propiedad utilizados para identificarla y los custodios responsables de esta. El examen efectuado el 31 de julio de 2009 sobre la información mantenida en los informes *Listado de Activos por Categoría y Localización – Hardware (Listado de Hardware)* y

Listado por Categoría Software (Listado de Software), producidos por el Módulo de Inventario reveló que la información mantenida en este sistema no era correcta y no estaba actualizada, según se indica:

1) Relacionado con el *Listado de Hardware*:

   a) No incluía tres computadoras[3] que fueron adquiridas por un monto de $3,081, mediante la Orden de Compra Núm. *CPN-10615* del 10 de junio de 2008.

   b) Incluía 52 equipos computadorizados[4], valorados en $41,462, los cuales aparecían asignados a 9 empleados que habían cesado labores en la Compañía, entre el 15 de diciembre de 2003 y el 31 de diciembre de 2008. Habían transcurrido entre 212 y 2,055 días desde la fecha de cese de estos empleados y la fecha del informe.

2) Relacionado con el *Listado de Software*:

   a) Incluía un servidor, un *T1 DSU Wan Interface Card*, un *UPS,* un *Etherfast* y un *zip drive*, valorados en $83,295, y los clasificaba como programas. Este informe debía limitarse a presentar programas computadorizados.

   b) No incluía el nombre de 18 programas[5] de la Compañía que estaban valorados en $43,146. Estos fueron identificados con la palabra *Programa* y correspondían a las licencias del Sistema *Oracle Financials*.

   c) No incluía el número de propiedad del programa *Visual Studio MS-Go* Pro.Ed, que estaba asignado a la OSI. Este programa estaba valorado en $750 y no pudo ser localizado en esta oficina. Durante nuestra inspección solo

---

[3] Los números de propiedad de las computadoras se incluyeron en el borrador de los **hallazgos** del *Informe* remitido al Director Ejecutivo para comentarios.

[4] Una relación de los equipos computadorizados se incluyó en en el borrador de los **hallazgos** del *Informe* remitido al Director Ejecutivo para comentarios.

[5] Los números de propiedad de los programas se incluyeron en el borrador de los **hallazgos** del *Informe* remitido al Director Ejecutivo para comentarios.

encontramos un programa *Studio 8*[6] y otro *Visual Studio* que había sido provisto por la OGP, el cual no se registraba en el Módulo de Inventario.

b. Al 20 de octubre de 2009, en la OSI no se mantenía un registro de los programas adquiridos e instalados en cada computadora de la Compañía que incluyera, entre otras cosas, lo siguiente:

- El número de licencias de los programas instalados
- El nombre del usuario
- El número de propiedad
- La descripción de la computadora en donde estaban instalados los programas.

Criterios

Las situaciones comentadas en el **apartado a.** se apartan de lo establecido en el Artículo VI del *Reglamento de Propiedad Mueble (Reglamento)*, según enmendado, aprobado el 9 de julio de 2003 por la Junta de Directores de la Compañía.

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico,* de la *Carta Circular Núm. 77-05*.

Efectos

Las situaciones que se comentan en el **apartado a.** no permiten a la Compañía mantener un control adecuado de la propiedad, lo que podría propiciar el uso indebido o la pérdida de la misma, sin que se puedan detectar a tiempo para fijar responsabilidades. Además, dificultan nuestra gestión fiscalizadora y le resta confiabilidad a la información existente en el Módulo de Inventario.

La situación comentada en el **apartado b.** impide ejercer un control eficaz de los programas y de las licencias de estos. Además, propicia la

[6] Véase la nota al calce 5.

instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la Compañía.

Causas

Las situaciones comentadas en el **apartado a.** se debieron a que la Directora de la Oficina de Administración, quien fungía como Encargada de la Propiedad:

- No cumplió con las disposiciones sobre el registro adecuado de la propiedad, establecidas en el *Reglamento.* **[Apartado a.1)a) y 2)]**
- No le había solicitado a la Ayudante Especial los cambios al *Módulo de Inventario*, necesarios para la reasignación de los equipos. **[Apartado a.1)b)]**

La situación comentada en el **apartado b.** se debía a que la Ayudante Especial no había tomado las medidas necesarias para mantener un registro de los programas instalados en las computadoras de la Compañía.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> [...] los números [...] no están registrados en el sistema. Se está haciendo la investigación pertinente en este asunto. [*sic*] **[Apartado a.1)a)]**
>
> Para poder arreglar este asunto se realizó un plan de trabajo donde se actualizará toda la aplicación de Activos Fijos para de esta manera poder actualizar la información de manera apropiada. [*sic*] **[Apartado a.1)b)]**
>
> Los siguientes números de propiedad fueron removidos del inventario [...] Los equipos con los números de propiedad [...] aún se encuentran en el listado de Software. Se solicitará a la Oficina de Propiedad que haga el cambio pertinente para corregir la situación. **[Apartado a.2)a)]**
>
> Estamos trabajando con el módulo de propiedad y se le solicitará a la Oficina de Propiedad que haga el cambio pertinente para corregir esta situación. **[Apartado a.2)b)]**

Véanse las recomendaciones 1, 3.d. y 7.

Hallazgo 5 - Deficiencias relacionadas con la producción y el almacenamiento de los respaldos de los archivos computadorizados de información

Situaciones

a. El examen realizado el 14 de octubre de 2009, relacionado con los procedimientos utilizados para la producción y el almacenamiento de los respaldos de los archivos computadorizados, mantenidos en los 18 servidores de la Compañía, reveló las siguientes deficiencias:

   1) Los respaldos diarios de la base de datos del *Sistema de Reservaciones* mantenida en uno de los servidores de la Compañía, no se realizaban en medios externos. Un Especialista de Recursos Humanos, que laboraba en la OSI en destaque, realizaba estos respaldos y los mantenía en el mismo servidor donde estaba la base de datos.

   2) El Oficial de Redes de Comunicación no realizaba los respaldos de los 18 servidores activos que estaban ubicados en el Cuarto de Servidores de la OSI. Estos servidores mantenían información relacionada con las finanzas, el control de la propiedad, la administración del personal, el correo electrónico, la página en Internet y la configuración de los sistemas utilizados. La Ayudante Especial solo mantenía en un disco externo un respaldo parcial del servidor donde estaba la base de datos del *Sistema de Reservaciones*. Este respaldo, el cual excluía dicha base de datos y sus respectivos respaldos, fue realizado el 11 de septiembre de 2009 y no se mantenía en un lugar seguro fuera de los predios de la Compañía.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Artículo 7, Sección 7.2 del *Manual de Acceso*.

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, entre otras cosas, que deberán existir procedimientos para tener y mantener un respaldo recurrente de la información y de los programas de aplicación

y de sistemas esenciales e importantes para las operaciones. En consonancia con dicha política pública se requiere producir respaldos de la información crítica de la Compañía y mantener una copia de estos almacenada en un lugar seguro fuera de los predios de la entidad y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre.

Efecto

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

Causas

Las situaciones comentadas se debían a que la unidad de respaldo utilizada por la Compañía estaba dañada hacía más de un año. Además, la Ayudante Especial no se aseguró de producir ni de mantener en un lugar externo una copia de los respaldos de la información mantenida en los sistemas computadorizados de la Compañía.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> En la actualidad la CPNPR adquirió una Unidad de *Backup* con capacidad de almacenamiento para 23 cartuchos magnéticos.[...] También se adquirió una aplicación para realizar los respaldos diariamente de todos los servidores de la CPNPR, los mismos son removidos de la unidad de *Backup* y son llevados fuera del Centro de Cómputos [...] y son mantenido bajo llave. [*sic*] **[Apartado a.1)]**
>
> En la actualidad el Oficial de Redes de Comunicación no realiza los respaldos de los 18 servidores de la CPNPR. Los respaldos son realizados por la Ayudante Especial, encargada de la OSI. **[Apartado a.2)]**

Véanse las recomendaciones 1 y 3.e.

Hallazgo 6 - Deficiencias relacionadas con los parámetros de control de acceso, y mantenimiento inadecuado de las cuentas de acceso

Situaciones

a. El examen realizado sobre los parámetros de control de acceso definidos en el servidor principal de la Compañía, reveló que al 9 de octubre de 2009, a 12 cuentas de acceso mantenidas en el servidor principal se les había configurado la opción que permitía a los usuarios mantener la misma contraseña indefinidamente (*password never expired).*

b. Al 10 de julio de 2009, no se habían desactivado las cuentas de acceso de 19 usuarios que no laboraban en la Compañía. Estos exempleados habían cesado sus funciones entre el 1 de marzo de 2003 y el 12 de enero de 2009, habían transcurrido entre 179 y 2,323 días desde la fecha de cese. Además, no se habían desactivado las cuentas de acceso asignadas a 2 usuarios que no pudieron ser identificados.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en el Artículo 8, Sección 8.2, *Solicitud de Acceso y Manejo a los Sistemas de Información (Contraseña)*, del *Manual de Acceso*. Además, la situación comentada en el **apartado b.** es contraria a lo establecido en el Artículo 7, Sección 7.3 de dicho *Manual*.

Efectos

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información, sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

La situación comentada en el **apartado a.** se debía a que la Ayudante Especial no se había asegurado de establecer en estas cuentas, la opción de seguridad para que las contraseñas de los usuarios expiraran cada 45 días, de acuerdo con lo establecido en el *Manual de Acceso*.

La situación comentada en el **apartado b.** se atribuye a la falta de comunicación efectiva entre la Oficina de Recursos Humanos, el área de trabajo del empleado y la OSI, para informar el cese de labores de los usuarios de los sistemas de información, de modo que los privilegios de acceso se mantuvieran actualizados.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> Las 12 cuentas con la contraseña en *password never expired* fueron cambiadas a las políticas del servidor principal donde la contraseña expira cada 60 días. A febrero de 2012 se han eliminado un total de 86 cuentas de acceso a la red. [*sic*] **[Apartados a. y b.]**

Véanse las recomendaciones 1, 3.f. y g., y 4.b.

Hallazgo 7 - Falta de un formulario para solicitar la modificación de los privilegios de las cuentas de acceso

Situación

a. El examen realizado entre el 21 de octubre de 2009 y el 5 de marzo de 2010, relacionado con los procedimientos utilizados para crear, modificar o eliminar las cuentas de acceso a los sistemas de información de la Compañía, reveló que la OSI no contaba con un formulario para solicitar la modificación de los privilegios de estas cuentas. El 5 de marzo de 2010, la Ayudante Especial nos certificó que los supervisores de los usuarios les solicitaban los cambios de las cuentas de acceso mediante una llamada telefónica o un correo electrónico que no era conservado.

Criterio

La situación comentada se aparta de 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. Se establece, además, que la información y los programas de aplicación utilizados en las operaciones de la agencia deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización. Esto se logra, en parte, mediante el establecimiento de controles de acceso rigurosos a la red, a los programas y a los archivos, incluido el uso de formularios para solicitar la modificación de las cuentas de acceso a los diferentes recursos disponibles a través de la red, para cada usuario.

Efectos

La situación comentada impide mantener la evidencia requerida de las autorizaciones para modificar los accesos y los privilegios a los usuarios. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y la utilicen indebidamente. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas sin que puedan ser detectadas a tiempo para fijar responsabilidades.

Causa

La situación comentada se debía a que la Ayudante Especial y el Director Auxiliar de Sistemas de Información no se habían percatado de la importancia de mantener un control adecuado de los accesos modificados y de documentar claramente la justificación de los mismos.

Véanse las recomendaciones 1 y 3.h.

Hallazgo 8 - Falta de normas y de procedimientos escritos para la administración y la seguridad de los sistemas computadorizados; de documentación sobre la entrega del Manual de Acceso; y de adiestramientos y pantallas de advertencias para concienciar sobre las normas establecidas para el uso y el control de los equipos y de los sistemas computadorizados

Situaciones

a. Al 4 de agosto de 2009, no se habían promulgado las normas ni los procedimientos escritos necesarios para reglamentar los siguientes procesos relacionados con la administración y la seguridad de los sistemas computadorizados:

- La creación y el mantenimiento de la información divulgada en la página electrónica
- La identificación, la selección, la instalación y la modificación de los sistemas operativos de las computadoras y de los servidores
- La identificación y la documentación de los problemas relacionados con las aplicaciones de los sistemas operativos y los incidentes de seguridad
- La administración de la red y el establecimiento de un registro de todos los programas instalados en esta y de un itinerario para el mantenimiento preventivo del equipo de la red
- La administración de la seguridad de los sistemas de bases de datos y el uso de programas utilitarios[7] para su administración
- La disposición de información sensitiva y de los programas, antes de transferir o dar de baja los equipos computadorizados y los medios de almacenamiento de información
- La otorgación de accesos remotos a los usuarios y consultores

[7] Programa especializado del sistema operativo utilizado para ejecutar funciones computadorizadas y rutinas particulares que se requieren con frecuencia en el curso normal del procesamiento.

- La adquisición, el desarrollo y el control de los cambios a las aplicaciones computadorizadas.

b. El Director Auxiliar de Sistemas de Información documentaba y tramitaba la entrega del *Manual de Acceso* a los usuarios de los sistemas de información mediante una hoja de trámite. El examen realizado el 14 de septiembre de 2009, sobre las hojas de trámite correspondientes a una muestra de 25 usuarios, reveló que para 16 de estos[8] (64 por ciento), en la OSI no se mantenía documentación que evidenciara la entrega del *Manual*.

c. La Compañía no había ofrecido adiestramientos periódicos sobre el uso y el control de los equipos y de los sistemas de información. Estos adiestramientos son necesarios para asegurarse de que el personal esté capacitado para ejercer sus funciones, utilizar y proteger los equipos adecuadamente, y cumplir con las responsabilidades relacionadas con la seguridad y la protección de la información registrada y accedida por este. La Oficina de Recursos Humanos nos certificó que, durante el período del 1 de octubre de 2007 al 1 de octubre de 2009, solo se le había ofrecido adiestramientos relacionados con aspectos técnicos a siete usuarios y a tres empleados de la OSI.

d. El examen realizado el 9 de octubre de 2009 a 20 computadoras[9] de la Compañía, reveló que estas no incluían una advertencia en la pantalla inicial para notificar a los usuarios sobre las normas principales para el uso de las mismas.

Criterios

La situación comentada en el **apartado a.** se aparta de lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establecen las directrices generales que permiten a las agencias implementar controles adecuados en sus sistemas de información

---

[8] Una relación de los usuarios se incluyó en el borrador de los **hallazgos** del *Informe* remitido al Director Ejecutivo para comentarios.

[9] Véase la nota al calce 3.

computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, se establece que será responsabilidad de cada entidad gubernamental desarrollar normas específicas que consideren las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y estén aprobados por la alta gerencia. Mediante los mismos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilitan el adiestramiento.

Las situaciones comentadas en los **apartados b. y d.** se apartan de lo establecido en la *Política Núm. TIG-008* de la *Carta Circular Núm. 77-05*. En esta se establece que cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad. Asimismo, será responsabilidad de cada entidad particular notificar debidamente a los empleados del contenido de las políticas internas establecidas para regular el uso de los sistemas de información de la entidad. Para esto, cada entidad gubernamental debe colocar un aviso que indique al usuario o a quien acceda el sistema de información que el mismo es propiedad de esa entidad del Estado Libre Asociado de Puerto Rico y que se compromete a utilizarlo conforme a las normas establecidas. Además, los usuarios firmarán un documento que indica que conocen la política y que cumplirán con esta.

Las situaciones comentadas en los **apartados del b. al d.** se aparta de lo establecido en el Artículo 7, Sección 7.2 del *Manual de Acceso.* En esta se establece, entre otras cosas, que la OSI deberá orientar y concienciar a los usuarios de los sistemas sobre las normas de seguridad, confidencialidad y protección de los equipos de la Compañía. Esto se logra, en parte, mediante la divulgación de las normas y de los procedimientos establecidos, un programa de adiestramiento continuo sobre la

reglamentación promulgada, y el uso de las pantallas de advertencias que permiten orientar y concienciar periódicamente al usuario sobre las normas para el uso de los sistemas de información.

Efectos

La situación comentada en el **apartado a.** podría ocasionar que las operaciones de los sistemas de información no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias. Además, podría exponer al personal de la OSI, los equipos y la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones y a otras situaciones adversas.

Las situaciones comentadas en los **apartados del b. al d.** podrían dar lugar a que los usuarios no observen las normas principales para el uso de los sistemas de información, y a que se dificulte imponer sanciones por violación a las mismas. Además, pueden provocar la comisión de irregularidades y otras situaciones adversas.

La situación comentada en el **apartado c.** puede propiciar, entre otras cosas, que no se utilicen al máximo los equipos y los programas computadorizados, se divulgue o pierda información almacenada en las computadoras, se utilicen equipos para funciones ajenas a la gestión pública, se utilicen programas computadorizados sin la debida autorización, y se instalen programas que no estén debidamente autorizados por la Compañía.

Causas

La situación comentada en el **apartado a.** obedece, principalmente, a que el Director Ejecutivo no le había requerido a la Ayudante Especial que desarrollara y remitiera para su consideración y para referido a la Junta de Directores, los procedimientos escritos necesarios para regular los procesos mencionados en este apartado.

La situación comentada en el **apartado b.** se atribuye, en parte, a que el Director Auxiliar de Sistemas de Información no veló porque el *Manual de*

Acceso fuera distribuido a todos los usuarios de los sistemas de información de la Compañía y porque se mantuviera documentación de todos los usuarios que lo recibieron.

La situación comentada en el **apartado c.** se atribuye a que la Directora de Recursos Humanos no había identificado las necesidades de adiestramientos que tenían los usuarios de los sistemas de información, a los fines de planificar, coordinar e implantar un plan de adiestramiento que los capacite en aspectos relacionados con el control y el uso de los equipos y los programas.

La situación comentada en el **apartado d.** se debía a que la Ayudante Especial no se había asegurado de que las advertencias fueran instaladas en todas las computadoras, como medida disuasiva para el uso oficial de los sistemas computadorizados.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> [...] Estamos trabajando para hacer todos los procedimientos escritos. **[Apartado a.]**
>
> El Manual de Acceso y Uso de los Sistemas de Información se encuentra en revisión en el cual se establecen nuevas normas, parámetros de seguridad y procedimientos para la administración de los sistemas de información. [*sic*] **[Apartado b.]**
>
> Una vez la Junta de Directores apruebe el manual de Acceso y Uso de los Sistemas de Información, se estará orientando a todo el personal sobre las normas del mismo. [*sic*] **[Apartado c.]**
>
> Estamos identificando las computadoras que están ubicadas fuera de la oficina central que no cuentan con la advertencia en la pantalla inicial sobre las normas principales para el uso de las mismas. [*sic*] **[Apartado d.]**

Véanse las recomendaciones 1, 3 de la i. a la k., y 4.c.

Hallazgo 9 - Falta de revisiones periódicas de los registros de eventos de los sistemas operativos y de los incidentes de seguridad de la red

Situaciones

a. Al 19 de agosto de 2009, la Ayudante Especial no suministró evidencia de que se realizaran verificaciones periódicas de los registros de eventos producidos por el sistema operativo del servidor principal y por los servidores que manejan los accesos a Internet y al correo electrónico.

b. Al 10 de septiembre de 2009, la Ayudante Especial nos certificó que no se mantenían registros de los incidentes de seguridad relacionados con la red, que incluyan información sobre los incidentes registrados, la documentación de las investigaciones realizadas y las medidas correctivas implementadas para evitar su ocurrencia.

Criterios

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. Además, se establece que todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes. Esta política se implementa, en parte, mediante la revisión continua, por el personal técnico especializado, de los registros computadorizados de eventos e incidentes de seguridad, producidos por los servidores principales.

Efectos

La situación comentada en el **apartado a.** priva a la OSI de información sobre errores en el sistema y posibles violaciones de seguridad que pudieran ocurrir en la red, que le permita tomar prontamente las medidas preventivas y correctivas necesarias.

La situación comentada en el **apartado b.** le impide a la OSI tener un control eficaz y documentado sobre las medidas preventivas y correctivas establecidas para el manejo de incidentes que afectan la operación y la

seguridad de los sistemas de información. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

Causa

Las situaciones comentadas se atribuyen a que la Ayudante Especial no se había asegurado de documentar el examen efectuado a los registros de los servidores principales y de mantener registros de los incidentes de seguridad de la red.

Comentarios de la Gerencia

El Director Ejecutivo informó en la carta que nos envió, entre otras cosas, lo siguiente:

> Para diciembre de 2010 se habilitó la función de *change tracking* al servidor de acceso al Internet para monitorear los cambios en la configuración, además, se utiliza la aplicación *Event Viewer* para el monitoreo de los sucesos del Sistema Operativo de todos los servidores que posee la CPNPR. [*sic*] **[Apartado a.]**
>
> Al momento no se mantienen registros sobre incidentes en la red. Pero estaremos trabajando con ello. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1 y 3.l.

RECOMENDACIONES

Al Presidente de la Junta de Directores de la Compañía de Parques Nacionales de Puerto Rico

1. Ver que el Director Ejecutivo de la Compañía cumpla con las **recomendaciones de la 2 a la 7** de este *Informe*. **[Hallazgos del 1 al 9]**

Al Director Ejecutivo de la Compañía de Parques Nacionales de Puerto Rico

2. Imparta instrucciones para que se realice 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 su revisión y para la aprobación de la Junta de Directores. **[Hallazgo 1]**

3. Ejercer una supervisión efectiva sobre la Ayudante Especial para asegurase de que:

   a. Redacte y remita para la consideración del Director Ejecutivo y para la aprobación de la Junta de Directores un plan de seguridad que incluya los criterios descritos en el **Hallazgo 2-a.** Una vez aprobado, asegurarse de que realicen pruebas periódicas y de que se divulgue a los empleados y a los funcionarios concernientes.

   b. Revise el *Plan de Contingencia para los Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico* para que incluya los requisitos necesarios para atender los aspectos comentados en el **Hallazgo 3-b.**, y lo remita para consideración del Director Ejecutivo y para la aprobación de la Junta de Directores.

   c. Efectúe las pruebas o los simulacros necesarios para verificar la efectividad del *Plan*, por lo menos, una vez al año y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 3-c.]**

   d. Mantenga un registro de los programas computadorizados de la Compañía. El registro deberá contener, entre otra información, el número de las licencias de los programas disponibles e instalados en las computadoras, el nombre del usuario, el número de propiedad y la descripción de la computadora donde están instalados los mismos. Esto, con el fin de mantener un inventario de los programas y de prevenir la instalación de programas no autorizados. **[Hallazgo 4-b.]**

   e. Se asegure de que una vez adquirida la unidad de respaldo, se realicen los respaldos de los sistemas de información en medios externos y se mantenga copias de estos en un lugar seguro fuera de los predios de la Compañía. **[Hallazgo 5]**

f. Se asegure de establecer la opción de seguridad para que las contraseñas de los usuarios expiren cada 45 días, de acuerdo con lo establecido en el *Manual de Acceso*. **[Hallazgo 6-a.]**

g. Se asegure, si aún no se ha realizado, de eliminar las cuentas de acceso de los exempleados mencionadas en el **Hallazgo 6-b.**

h. Cree un formulario para la modificación de los privilegios otorgados a los usuarios, que permita mantener un control adecuado de los mismos. **[Hallazgo 7]**

i. Redacte y remita para la consideración del Director Ejecutivo, las normas y los procedimientos necesarios para reglamentar los procesos que se indican en el **Hallazgo 8-a.** Una vez evaluados, las normas y los procedimientos deben ser referidos a la Junta de Directores para su aprobación.

j. Se asegure de que se distribuya a todos los usuarios de los sistemas de información de la Compañía el *Manual de Acceso*. Una vez distribuido, se asegure de conservar los recibos de entrega firmados por los usuarios para mantener evidencia de este trámite. **[Hallazgo 8-b.]**

k. Incluya una advertencia en la pantalla inicial de todas las computadoras para que se notifique a los usuarios sobre las normas principales para el uso de las mismas y estos se comprometan a observarlas, y conozcan las medidas aplicables en caso de violación a las mismas. **[Hallazgo 8-d.]**

l. Mantenga la documentación del examen efectuado a los registros de eventos producidos en los servidores principales de la Compañía y a los registros de los incidentes de la red. Esta documentación debe incluir las medidas correctivas y preventivas implementadas para prevenir y corregir los errores del sistema, los eventos no autorizados de las aplicaciones y el uso indebido de los sistemas de información. **[Hallazgo 9]**

4. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para que:

   a. Se asegure de proveer a los empleados el *Acuerdo* y cumpla con las directrices para el trámite y el manejo del mismo, según establecido en el *Manual de Acceso*. **[Hallazgo 2-b.]**

   b. Se asegure de informar prontamente a la OSI el cese de los empleados para la cancelación de sus cuentas de acceso. **[Hallazgo 6-b.]**

   c. Realice un estudio de las necesidades de adiestramiento que tienen los usuarios, y planifique, coordine e implemente un plan de adiestramiento que los capacite en aspectos relacionados con el control y el uso de los equipos y los sistemas. **[Hallazgo 8-c.]**

5. Realizar las gestiones pertinentes para asegurarse de que se prepare un plan de continuidad de negocios que cumpla con lo requerido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. El mismo debe ser remitido para revisión y aprobación de la Junta de Directores. Una vez sea aprobado, tomar las medidas necesarias para asegurarse de que se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Compañía. Además, asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicamente para garantizar su efectividad. **[Hallazgo 3-a.]**

6. Formalizar un acuerdo escrito con otra entidad que acepte la utilización de sus respectivos equipos en casos de desastres o emergencias en la Compañía, o considerar establecer su propio centro alterno en alguna de sus instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 3-d.]**

7. Ver que la Directora de la Oficina de Administración:

   a. Cumpla con las disposiciones sobre el registro adecuado de la propiedad, establecidas en el *Reglamento*. **[Hallazgo 4-a.1)a) y 2)]**

   b. Solicite a la Ayudante Especial los cambios al *Módulo de Inventario* necesarios para la reasignación de los equipos. **[Hallazgo 4-a.1)b)]**

AGRADECIMIENTO

A los funcionarios y a los empleados la Compañía de Parques Nacionales de Puerto Rico, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor

Por: Yesmín M. Valdivieso

ANEJO 1

COMPAÑÍA DE PARQUES NACIONALES DE PUERTO RICO

OFICINA DE SISTEMAS DE INFORMACIÓN

MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Henry Neumann Zayas	Presidente	19 jun. 09	5 mar. 10
Ing. Jaime López	Director Ejecutivo de la Compañía de Turismo de Puerto Rico	19 jun. 09	5 mar. 10
Arq. Psj. Juan J. Terrasa Soler	Director Auxiliar de Planificación de la Compañía de Turismo de Puerto Rico	19 jun. 09	5 mar. 10
Dr. Reinaldo del Valle Cruz	Ayudante Especial de la[10] Secretaria del Departamento de Educación	9 feb. 10	5 mar. 10
Hon. Edward Moreno Alonso	Secretario Asociado del Departamento de Educación	19 jun. 09	17 dic. 09

[10] El Departamento de Educación no tuvo representación en la Junta de Directores durante el período del 18 de diciembre de 2009 al 8 de febrero de 2010.

ANEJO 2

COMPAÑÍA DE PARQUES NACIONALES DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Daniel J. Galán Kercadó	Secretario de Recursos Naturales y Ambientales y Director Ejecutivo	19 jun. 09	5 mar. 10
Sra. Felícita Pizarro Calderón	Directora de Finanzas y Presupuesto	19 jun. 09	5 mar. 10
Sra. Yolanda Fonseca Torres	Directora de Administración	16 jul. 09	5 mar. 10
Sra. Clara Arriaga Correa	"[11]	19 jun. 09	15 jul. 09
Sra. Susan I. Peña De Jesús	Directora de Recursos Humanos	19 jun. 09	5 mar. 10
Srta. Lymary Maymí Barreto	Ayudante Especial[12]	2 jul. 09	5 mar. 10
Sr. Daniel González Ruiz	Director Auxiliar de Sistemas de Información	19 jun. 09	5 mar. 10

[11] El puesto de Directora de Administración estuvo vacante del 19 de junio al 15 de julio de 2009. Durante dicho período, las funciones del indicado puesto fueron ejercidas por la señora Arriaga Correa, pero con el puesto de carrera de Directora Auxiliar de Administración.

[12] El puesto de Director de Sistemas de Información estuvo vacante del 19 de junio de 2009 al 5 de marzo de 2010. Durante el período del 2 de julio de 2009 al 5 de marzo de 2010, las funciones del indicado puesto fueron ejercidas por la señorita Maymí Barreto, pero con el puesto de Ayudante Especial.

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