Secretaría

Lcda. Tania Barbarossa Ortiz

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

Senado
DE PUERTO RICO

El Capitolio
PO Box 9023431
San Juan, Puerto Rico
00902-3431

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

REFERIDO A:

COMISIONES PERMANENTES

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

COMISIONES ESPECIALES

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

COMISIONES CONJUNTAS

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

#856.

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

27-febrero-2013

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

27 de febrero de 2013

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

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

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-13-13* de la Oficina de Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico, aprobado por esta Oficina el 10 de febrero de 2013. Publicaremos dicho *Informe* en nuestra página en Internet: http://www.ocpr.gov.pr para conocimiento de los medios de comunicación y de otras partes interesadas.

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

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

Cordialmente,

Yesmín M. Valdivieso

Yesmín M. Valdivieso

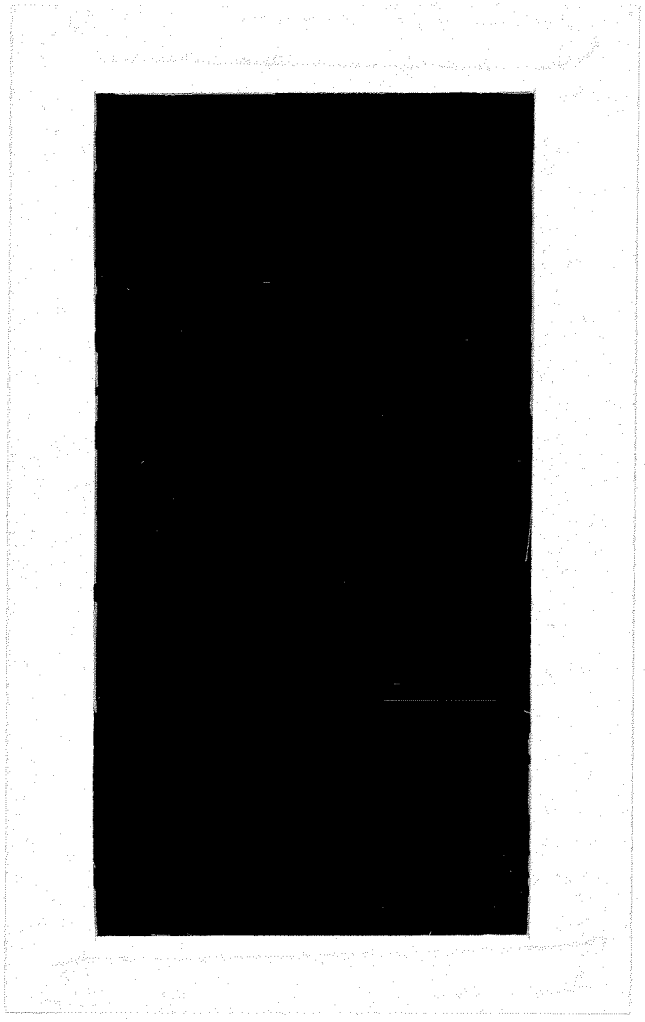
Anejo

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

#856

[redacted]

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



INFORME DE AUDITORÍA TI-13-13

10 de febrero de 2013

Compañía de Parques Nacionales de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5212 - Auditoría 13308)

Período auditado: 19 de junio de 2009 al 15 de julio de 2010

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **5**

OPINIÓN Y HALLAZGOS **6**

1 - Deficiencias relacionadas con la administración de las cuentas de acceso activas en la tabla de seguridad de la base de datos Reservaciones 6

2 - Falta de segregación de las funciones realizadas por un Desarrollador de Sistemas de Informática, y de las tareas que podían realizar en el Sistema de Ventas los usuarios que tenían nivel de acceso de administrador 10

3 - Deficiencias relacionadas con la programación de los parámetros de seguridad del Sistema de Ventas y el sistema Reservaciones de Cabañas y Villas 15

4 - Falta de un registro sobre los cambios efectuados a la información contenida en la base de datos de Reservaciones 19

5 - Documentación incompleta del Sistema de Ventas, del sistema Reservaciones de Cabañas y Villas y del Sistema Reservaciones-Internet, y deficiencias en el Manual Sistema de Reservaciones 20

RECOMENDACIONES **25**

AGRADECIMIENTO **28**

ANEJO 1 - INFORME PUBLICADO **29**

ANEJO 2 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **30**

ANEJO 3 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **31**

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

10 de febrero de 2013

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Compañía de Parques Nacionales de Puerto Rico (Compañía) para determinar si se efectuaron de acuerdo con las normas generalmente aceptadas en este campo, y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 19 de junio de 2009 al 15 de julio de 2010. En algunos aspectos se examinaron transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este es el segundo informe, y contiene cinco hallazgos sobre el resultado del examen que realizamos de los controles para la documentación y el acceso al *Sistema de Ventas*, al sistema *Reservaciones de Cabañas y Villas*, al *Sistema Reservaciones-Internet*, y a la base de datos *Reservaciones* de la Compañía. En el **ANEJO 1** presentamos información del informe emitido sobre 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. Ambos informes están disponibles en nuestra página en Internet: http://www.ocpr.gov.pr.

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. En la *Ley 10-2001* se dispuso que la Compañía operará un sistema que integre todos los parques naturales, recreativos o 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 será el Presidente de la Junta. Además, 3 de los miembros serán 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 responde 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 2 y 3** 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, y 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[1], 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 fiscales 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[2].

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 Sr. Daniel J. Galán Kercadó, entonces Secretario de Recursos Naturales y Ambientales y Director Ejecutivo de la Compañía, mediante carta de nuestros auditores, del 10 de agosto de 2010. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

---

[1] La titularidad del Parque Luis Muñoz Marín fue transferida al Municipio de San Juan mediante la *Resolución Conjunta 180* aprobada el 30 de diciembre de 2010.

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

Mediante carta del 23 de agosto de 2010, el señor Galán Kercadó remitió sus comentarios a los hallazgos incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al entonces Secretario de Recursos Naturales y Ambientales y Director Ejecutivo de la Compañía, para comentarios, por carta del 15 de noviembre de 2012.

El entonces Secretario de Recursos Naturales y Ambientales y Director Ejecutivo contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 28 de noviembre de 2012. Sus comentarios se consideraron en la redacción final de este *Informe*; y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**. Luego de evaluar dichos comentarios y la evidencia suministrada, determinamos que la Compañía tomó las acciones correctivas pertinentes, excepto por los **hallazgos** que se incluyen en este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a los controles para la documentación y el acceso al *Sistema de Ventas*, el sistema *Reservaciones de Cabañas y Villas*, el *Sistema Reservaciones-Internet* y la base de datos *Reservaciones* de la Compañía, se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 5** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con la administración de las cuentas de acceso activas en la tabla de seguridad de la base de datos Reservaciones

Situaciones

a. Los ingresos de la Compañía provienen en su mayoría de los pagos recibidos por concepto de las reservaciones de las instalaciones ubicadas en sus centros vacacionales, balnearios, parques y áreas recreativas. Para contabilizar estos ingresos y controlar el proceso de las reservaciones, desde el 2001 la Compañía contaba con el sistema *Reservaciones de Cabañas y Villas*, y desde el 2008 con

el *Sistema de Ventas*. Además, contaba con el *Sistema Reservaciones-Internet* que le permitía a los ciudadanos efectuar reservaciones de las instalaciones a través de la página electrónica de la Compañía.

Los tres sistemas de reservaciones eran utilizados concurrentemente para registrar las transacciones relacionadas con las reservaciones de las instalaciones de la Compañía y efectuar el cobro correspondiente. Las transacciones registradas por los tres sistemas de reservaciones actualizaban la base de datos *Reservaciones*. Estos sistemas asignaban automáticamente un número de confirmación a cada reservación que permitía identificar el sistema en que fue procesada la transacción.

El sistema *Reservaciones de Cabañas y Villas* fue desarrollado por el Desarrollador de Sistemas de Informática de la OSI. Este sistema debió ser sustituido en el 2008 por el *Sistema de Ventas*. Sin embargo, este último no permitía realizar consultas de las reservaciones efectuadas en el sistema *Reservaciones de Cabañas y Villas*, y no incluía opciones para procesar las excepciones de créditos y algunas transacciones de grupo. Por esto, se determinó que a partir del 2 de julio de 2010 se continuaría con el sistema *Reservaciones de Cabañas y Villas* el cual sería utilizado solamente por cinco usuarios autorizados[3].

El *Sistema de Ventas* también fue diseñado por el Desarrollador de Sistemas de Informática de la OSI. Este sistema comenzó a utilizarse el 4 de abril de 2008 y era utilizado por el personal que laboraba en la Oficina de Reservaciones[4] de la Oficina Central, en los centros vacacionales de la Compañía y en algunos balnearios, parques y áreas recreativas, para procesar las transacciones de reservaciones de las

---

[3] Los puestos de los usuarios autorizados se incluyeron en el borrador de los **hallazgos** del *Informe* remitido al entonces Director Ejecutivo para comentarios.

[4] La Oficina de Reservaciones formaba parte de la Oficina de Mercadeo y Servicio al Cliente de la Compañía. Esta oficina estaba a cargo de procesar las reservaciones a nivel central, preparar informes de las ventas y atender reclamaciones, entre otros.

cabañas y villas; y para procesar los pagos por concepto de la renta de cabañas, de villas, de salones de actividades, de pérgolas, de pabellones y de gazebos.

El *Sistema Reservaciones-Internet* permitía al público realizar sus reservaciones y pagos de forma electrónica, mediante el uso de tarjetas de crédito. Para esto, el usuario debía acceder el sistema mediante el enlace https://www.cpnpr.com, completar su reservación y emitir el pago total de la misma.

Las cuentas utilizadas para acceder a los tres sistemas de reservaciones estaban definidas en la tabla de seguridad de la base de datos *Reservaciones*. En esta tabla de seguridad se habían creado niveles de acceso de administrador (administrador completo y administrador limitado), supervisor (supervisor completo y supervisor limitado), usuario (usuario R/W completo y usuario R/W limitado), y usuario consulta (usuario R completo, y usuario R limitado). Estos niveles definían el privilegio de acceso de cada usuario.

El examen efectuado el 14 de diciembre de 2009 sobre los privilegios de 175 cuentas de acceso que se encontraban activas en la tabla de seguridad de la base de datos *Reservaciones*, y de la información mantenida sobre los usuarios de estas cuentas, reveló las siguientes deficiencias:

1) No se habían deshabilitado 11 cuentas de acceso[5] de empleados que habían cesado sus funciones entre el 15 de julio de 2002 y el 12 de enero de 2009, según las certificaciones provistas por la Directora de Recursos Humanos. A la fecha del examen, habían transcurrido entre 336 y 2,668 días desde la fecha de cese.

---

[5] Una relación de las cuentas de acceso se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al entonces Director Ejecutivo para comentarios.

2) A dos cuentas de acceso[6] asignadas a un Superintendente Asociado de Parques, a una cuenta[6] asignada a una Asistente Administrativo y a una cuenta[6] asignada a una Analista de Contabilidad, se les había otorgado el privilegio de usuario el cual permitía, entre otras cosas, crear clientes, y registrar y consultar reservaciones. Esto, a pesar de que dichos empleados no realizaban funciones relacionadas con el trámite de las reservaciones.

Criterios

Las situaciones comentadas son contrarias a lo establecido en los artículos 7 y 8 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.

Efectos

La situación comentada en el **apartado a.1)** dio lugar a que dos cuentas de acceso[6] de empleados que habían cesado sus funciones en la Compañía fueran utilizadas en fechas posteriores al cese de estos, para registrar transacciones de venta de reservaciones en la base de datos *Reservaciones*.

La situación comentada en el **apartado a.2)** propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propicia la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de la Compañía, sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

La situación comentada en el **apartado a.1)** se atribuye a la falta de comunicación efectiva entre la Oficina de Recursos Humanos y la OSI,

---

[6] Los nombres de la cuentas de acceso se incluyeron en el borrador de los **hallazgos** del *Informe* remitido al entonces Director Ejecutivo para comentarios.

para informar el cese de labores de los usuarios de los sistemas de información, de modo que los privilegios de acceso se mantuvieran actualizados.

La situación comentada en el **apartado a.2)** se debe a que la Ayudante Especial no se había asegurado de que se revisaran y actualizaran periódicamente los accesos otorgados al sistema *Reservaciones de Cabañas y Villas* y al *Sistema de Ventas*.

Comentarios de la Gerencia

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

> Para corregir esta situación, se añadió en la hoja de separación de deberes de la CPN un renglón dirigido a la Oficina de Sistemas de Información, este se utiliza para verificar todas las cuentas de accesos a los diferentes sistemas que posee la CPN, una vez verificado se procede a firmar el documento. [*sic*] **[Apartado a.1)]**
>
> En la actualidad hay 89 cuentas desactivadas. Incluyendo las que son mencionadas. [*sic*] **[Apartado a.1)]**
>
> En la actualidad, se añadió al sistema de seguridad un área que permite otorgar privilegios a todos los usuarios de manera independiente según sea solicitado por el supervisor o el Director Ejecutivo. Las cuentas de [...] fueron desactivadas. **[Apartado a.2)]**

Véanse las recomendaciones de la 1 a la 3.b.

Hallazgo 2 - Falta de segregación de las funciones realizadas por un Desarrollador de Sistemas de Informática, y de las tareas que podían realizar en el Sistema de Ventas los usuarios que tenían nivel de acceso de administrador

Situaciones

a. Al 20 de octubre de 2009, el Desarrollador de Sistemas de Informática, realizaba funciones propias de un programador que incluía, entre otras, crear y modificar la programación de los sistemas de la Compañía. Además, utilizaba dos de las cuatro cuentas de

acceso[7] que tenía asignadas para realizar otras funciones que resultaban conflictivas e incompatibles con las que efectuaba como parte de los deberes de su puesto, ya que le permitían:

- Acceder a la base de datos *Reservaciones* que estaba en producción, y modificar su esquema, su estructura y su seguridad. Estas funciones eran propias de un administrador de base de datos[8].

- Modificar mediante un programa utilitario de administración de base de datos, la información de los clientes y las reservaciones efectuadas por estos, las cuales se mantenían grabadas en las tablas de la base de datos *Reservaciones.* Esta función debía ser efectuada, sólo en casos excepcionales y de forma controlada, por el dueño de los datos de reservaciones, y validada por un administrador de base de datos.

- Acceder como usuario en ambiente de producción, al sistema *Reservaciones de Cabañas y Villas* y al *Sistema de Ventas*, e ingresar transacciones que actualizaban la base de datos *Reservaciones*.

- Crear y modificar las cuentas de acceso de los usuarios del sistema *Reservaciones de Cabañas y Villas* y el *Sistema de Ventas*. Esta función debía ser efectuada por el Oficial de Redes de Comunicación, luego de ser autorizada por la Directora de la Oficina de Mercadeo y Servicio al Cliente y la Ayudante Especial.

- Acceder a la programación del *Sistema de Ventas* que estaba en ambiente de producción para instalarle nuevos procedimientos de programación y modificar los existentes. La instalación de

---

[7] Véase la nota al calce 6.

[8] A la fecha de nuestra auditoría, la Compañía no contaba con un puesto de administrador de base de datos por lo que estas funciones debían ser asignadas a otro empleado de la OSI que no realizara funciones incompatibles. Además, debían establecerse medidas de supervisión que garantizaran que las funciones efectuadas por el empleado asignado fueran correctas y autorizadas.

procedimientos de programación, nuevos o modificados, debía ser efectuada por el Oficial de Redes de Comunicación, luego de ser debidamente probados en ambiente de prueba y autorizados por la Ayudante Especial.

Esta situación se agravaba al no existir un control alterno de supervisión por parte de la Ayudante Especial sobre las tareas de este empleado, ni un registro de auditoría que incluyera información sobre los cambios efectuados a la información contenida en la base de datos *Reservaciones*. **[Hallazgo 5]**

b. Al 14 de diciembre de 2009, existían 13 usuarios que tenían 14 cuentas[9] con niveles de acceso de administrador (administrador completo y administrador limitado). Estas cuentas eran utilizadas por personal de la OSI y por personal administrativo de la Oficina de Reservaciones.

El examen realizado sobre estos niveles de acceso reveló que, además de los privilegios relacionados con la administración de la seguridad, dichos niveles de acceso tenían asignados privilegios relacionados con el procesamiento de las transacciones de reservaciones que le permitían a los usuarios efectuar las siguientes tareas:

- Registrar y cancelar las reservaciones.
- Añadir, buscar, editar y eliminar la información personal del cliente.
- Liberar unidades relacionadas con transacciones que no fueron procesadas.
- Añadir, buscar, editar y eliminar reservaciones de grupos.
- Transferir clientes a los grupos.
- Definir los conceptos de ventas en las instalaciones.

---

[9] Los nombres de la cuentas de acceso, dos de las cuales estaban asignadas al Desarrollador de Sistemas de Informática, se incluyeron en el borrador de los **hallazgos** del *Informe* remitido al entonces Director Ejecutivo para comentarios.

- Bloquear y liberar unidades bloqueadas en las instalaciones.
- Eliminar recibos de otros conceptos de ventas de la Compañía.
- Configurar las ofertas para promover las reservaciones de las instalaciones.
- Transferir los créditos otorgados mediante el sistema *Reservaciones de Cabañas y Villas*.

Estas tareas eran incompatibles con las relacionadas con la administración de la seguridad, que son propias de las cuentas con niveles de acceso de administrador.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Artículo 8 del *Manual de Acceso*. En este se establece que el acceso de los empleados o los usuarios de los sistemas de información de la Compañía se determinará de acuerdo con las funciones, las responsabilidades y los deberes del puesto que ocupa.

Además, 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. En esta se establece que las agencias deberán implantar controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Conforme a dicha política y como norma de sana administración, es necesario que se segreguen las funciones relacionadas con las operaciones de los sistemas de información de la entidad, o se establezca la supervisión de las que resultan conflictivas, como control compensatorio. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades y que no se detecten a tiempo.

Efecto

Las situaciones comentadas pueden propiciar que se realicen transacciones no autorizadas en los archivos de los sistemas, que se cometan errores e irregularidades y que no se puedan detectar con prontitud, con los consiguientes efectos adversos para la Compañía.

Causas

Las situaciones comentadas se atribuyen a que la Ayudante Especial no se había asegurado de mantener una segregación y supervisión adecuadas sobre las funciones realizadas por el Desarrollador de Sistemas de Informática. **[Apartado a.]** Además, no se aseguró de que este evaluara los niveles de acceso diseñados en la programación del *Sistema de Ventas* y en la base de datos *Reservaciones* para que incluyera los niveles de acceso necesarios que permitieran una segregación de deberes adecuada entre la administración de la seguridad y el procesamiento de las transacciones del *Sistema de Ventas* y del sistema *Reservaciones de Cabañas y Villas*. **[Apartado b.]**

Comentarios de la Gerencia

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

> La CPN no cuenta con un puesto de Administrador de Sistemas o Base de datos disponibles. La política pública redujo el número de puestos para empleados de carrera y las funciones de éstos tuvieron que ser distribuidas entre los funcionarios de mayor experiencia y capacitación. Sin embargo, se solicitará a la Oficina de Recursos Humanos un análisis de esta situación para identificar dentro de los recursos de OSI o la Compañía si existe un funcionario que reúna los requisitos para ocupar el puesto de Administrador de Sistema para solucionar este señalamiento. [*sic*] **[Apartado a.1)]**
>
> En estas cuentas con nivel de acceso de administrador no tienen todos los accesos activados, se desarrolló una manera de poder restringir áreas del sistema al que solo los administradores tienen acceso. [*sic*] **[Apartado a.2)]**

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

Hallazgo 3 - Deficiencias relacionadas con la programación de los parámetros de seguridad del Sistema de Ventas y el sistema Reservaciones de Cabañas y Villas

Situaciones

a. El examen efectuado entre el 14 de diciembre de 2009 y el 16 de marzo de 2010 sobre la programación de los parámetros para la seguridad en el *Sistema de Ventas* y el sistema *Reservaciones de Cabañas y Villas*, reveló las siguientes deficiencias:

1) Al 16 de marzo de 2010, en el *Sistema de Ventas* no se había establecido mediante programación una opción para requerir el cambio periódico de las contraseñas de los 13 usuarios que tenían el privilegio de administrador, el cual le permitía acceder la pantalla de seguridad.

2) Al 14 de diciembre de 2009, el Desarrollador de Sistemas de Informática no había implementado en la programación del *Sistema de Ventas* y del sistema *Reservaciones de Cabañas y Villas*, el uso de un sistema de algoritmo seguro para encriptar[10] y proteger las contraseñas de los usuarios de estos sistemas.

3) El Desarrollador de Sistemas de Informática no había incluido instrucciones en la programación del *Sistema de Ventas* y del sistema *Reservaciones de Cabañas y Villas* que requirieran el uso de contraseñas definidas mediante la combinación de letras, números y caracteres especiales. En el examen realizado determinamos que, al 14 de diciembre de 2009, en la tabla de seguridad de la base de datos *Reservaciones* se mantenían 181 cuentas[11] de acceso activas e inactivas, cuyas contraseñas no eran seguras.

---

[10] La encripción es el proceso de convertir la información que está en formato texto en un código secreto mediante la utilización de algoritmos seguros. Para poder leer el mensaje, se requiere tener acceso a una llave secreta cuando se utiliza la encripción simétrica y a dos llaves cuando se utiliza la encripción asimétrica. Entre los algoritmos seguros utilizados se encuentran el SHA-1 y el MD-5.

[11] Al 14 de diciembre de 2009, en la tabla de seguridad se mantenían 175 cuentas de acceso activas y 6 inactivas.

4) El *Sistema de Ventas* y el sistema *Reservaciones de Cabañas y Villas* asignaban de forma secuencial un número de usuario que era único para cada cuenta de acceso creada en la tabla de seguridad de la base de datos *Reservaciones*. Este número era necesario para:

- Identificar en la tabla *Transacciones*, los usuarios que habían efectuado alguna transacción en el sistema *Reservaciones de Cabañas y Villas*.
- Acceder mediante las pantallas *Consulta por Recibo* del *Sistema de Ventas*, la información sobre las transacciones de pagos que habían sido registradas por los usuarios. Esta información no podía ser accedida cuando en la tabla de seguridad no existía el número de usuario y sólo un usuario había efectuado las transacciones relacionadas con la reservación consultada.
- Acceder mediante la pantalla *Selección de Reportes* del *Sistema de Ventas*, la información sobre las transacciones de pagos registradas por cada usuario, que se incluían en el *Informe Diario por Cajero*. Cuando no existía la información del usuario en la tabla de seguridad, su nombre no aparecía entre los nombres disponibles para producir este informe.

El examen efectuado el 14 de diciembre de 2009 sobre la tabla de seguridad reveló que se habían eliminado las cuentas de acceso relacionadas con 54 números de usuario. Estas debían mantenerse para poder tener acceso a la información histórica de los usuarios que habían efectuado transacciones contenidas en la base de datos. Estos números formaban parte de la secuencia numérica entre 2[12] y 236 que correspondían a las 181 cuentas de acceso incluidas en esta tabla.

---

[12] Los números de usuarios asignados en la tabla iniciaban en 2. Durante la auditoría no se pudo determinar si el número de usuario 1 existió.

Criterios

Las situaciones comentadas en el **apartado a.1), 3) y 4)** son contrarias a lo establecido en el Artículo 7 del *Manual de Acceso*. En este se establece que la OSI tendrá a su cargo todo lo relativo al acceso de los sistemas de información; que deberá mantener un registro que incluya, entre otras cosas, el nombre de los usuarios a los cuales se les ha otorgado el acceso; y que deberá establecer los mecanismos para que las claves de acceso sean renovadas cada 45 días y que contengan al menos 7 caracteres, entre los cuales debe incluir una letra, un número y un carácter especial.

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 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 la seguridad de la información deberá ser parte integral de cualquier programa de aplicación que adquiera o desarrolle la agencia para facilitar sus operaciones o mejorar el servicio de los ciudadanos. Esta política se implanta mediante el uso de contraseñas complejas para acceder a los sistemas de información, el cambio periódico de las contraseñas, la protección de las mismas, y la documentación completa y actualizada de los usuarios a los que se les ha otorgado privilegios para acceder los sistemas.

Efectos

La situaciones comentadas en los **apartados a. del 1) al 3)** propician que personas no autorizadas puedan acceder a la información confidencial del sistema *Reservaciones de Cabañas y Villas* y del *Sistema de Ventas*, y hacer uso indebido de esta. Además, podría ocasionar el registro, la eliminación o la modificación de información sobre las transacciones de reservaciones, lo que afectaría la confiabilidad e integridad de estas.

La situación comentada en el **apartado a.4)** limitó nuestro alcance para identificar el nombre de cuatro usuarios con cuyas cuentas de acceso[13] se habían registrado transacciones de cobro por un total de $504,324[14].

Además, la situación comentada limitó nuestro alcance para identificar un usuario que el 3 de junio de 2009 había accedido el sistema *Reservaciones de Cabañas y Villas* mediante el número de usuario 208 y tenía eventos registrados en la tabla *Transacciones*.

Causas

Las situaciones comentadas se debían a que la Ayudante Especial y el Director Auxiliar de Sistemas de Información no requirieron al Desarrollador de Sistemas de Informática que incluyera en el diseño del sistema *Reservaciones de Cabañas y Villas* y del *Sistema de Ventas*, los controles necesarios para corregir las situaciones comentadas en el **apartado a. del 1) al 3)** y, para garantizar la seguridad, la integridad y la confiabilidad de la información relacionada con el trámite de las reservaciones. Además, el Desarrollador de Sistemas de Informática no había alertado sobre los efectos de la eliminación de las cuentas de acceso en la disponibilidad de la información de los usuarios. **[Apartado a.4)]**

Comentarios de la Gerencia

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

> El implemento desarrollado dentro de la programación del Sistema de Ventas para que las contraseñas de acceso tuvieran al menos siete caracteres entre estos números, letras y un carácter especial no está encriptado. [*sic*] **[Apartado a.2)]**

---

[13] Véase la nota al calce 6.

[14] Las transacciones registradas por estos usuarios se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al entonces Director Ejecutivo para comentarios.

> Se implementó dentro de la programación del Sistema de Ventas el que las contraseñas de acceso tuvieran al menos 7 caracteres, entre estos: números, letras y un carácter especial. [*sic*] **[Apartado a.3)]**
>
> No hay registro alguno de lo que ocurrió con las cuentas eliminadas de la tabla de seguridad. [*sic*] **[Apartado a.4)]**

Véanse las recomendaciones 1 y 3 de la d.2) a la 4).

Hallazgo 4 - Falta de un registro sobre los cambios efectuados a la información contenida en la base de datos de Reservaciones

Situación

a. Al 1 de julio de 2010, la Compañía no mantenía un registro, mediante un programa de administración de bases de datos, de los cambios efectuados a la información contenida en la base de datos *Reservaciones* por el Desarrollador de Sistemas de Informática, el Especialista de Recursos Humanos que había sido autorizado a trabajar en la OSI, y una Analista de Mercadeo y Servicio al Cliente. El registro de auditoría que se mantenía sólo incluía información sobre el encendido, el apagado y las operaciones diarias del servidor, incluida la preparación de los respaldos.

Criterio

La situación comentada es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establece que deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten. Esta política se instrumenta, en parte, mediante la producción de registros de auditoría sobre los cambios efectuados en los sistemas de información, y el examen continuo de estos.

Efectos

La situación comentada priva a los supervisores y a los auditores de una herramienta necesaria para detectar cambios incorrectos o no autorizados, e investigar cualquier excepción en la base de datos *Reservaciones*. Además, dificulta fijar responsabilidades en los casos que procedan.

Causa

La situación comentada se debía a que la Ayudante Especial y el Director Auxiliar de Sistemas de Información no se aseguraron de que se estableciera el registro de auditoría comentado.

Comentarios de la Gerencia

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

> El registro de auditorías del servidor registra eventos del sistema, seguridad, Respaldos y otras aplicaciones en el servidor. El mismo se mantiene en una herramienta [...] [*sic*]

Consideramos las alegaciones del entonces Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que la herramienta utilizada no provee información detallada de las transacciones efectuadas por los usuarios en la base de datos.

Véanse las recomendaciones 1 y 3.f.

Hallazgo 5 - Documentación incompleta del Sistema de Ventas, del sistema Reservaciones de Cabañas y Villas y del Sistema Reservaciones-Internet, y deficiencias en el Manual Sistema de Reservaciones

Situaciones

a. Al 1 de octubre de 2009, la documentación del *Sistema de Ventas*, del sistema *Reservaciones de Cabañas y Villas* y del *Sistema Reservaciones–Internet* (sistemas de reservaciones) no incluía lo siguiente:

   1) Los diagramas de flujo sobre los procesos en línea (*online*), que detallen el nombre de los procesos, de las bases de datos y de los archivos afectados por cada transacción, y de los informes producto de estos.

   2) Un manual del programador que contenga una descripción general sobre los programas de los sistemas y su funcionalidad.

   3) La evidencia de los cambios efectuados a los programas y a la estructura de la base de datos *Reservaciones*, que incluya la

solicitud, la autorización, la asignación del programador y las pruebas de estos cambios, así como la autorización para mover los mismos al ambiente de producción.

4) Un manual del operador o guía técnica que incluya información para orientar al personal de la OSI sobre los requisitos mínimos necesarios para la operación de los sistemas, los registros de auditoría disponibles, la creación de las cuentas de acceso, los criterios para otorgar privilegios a estas, las conexiones internas y externas requeridas, y la configuración de la seguridad.

5) Un diccionario de datos (*Data Dictionary*)[15] que contenga lo siguiente:

- La descripción de los elementos de datos[16] (*data element definition*)
- Los valores preestablecidos a los elementos de datos (*data element default values*)
- El formato requerido por diseño para los elementos de datos (*data element edit mask*)
- La explicación de los códigos y las reglas de validación para los elementos de datos (*data element coding*)
- La referencia a tablas donde los elementos son utilizados y su rol como elemento de datos primario o secundario
- Una descripción de la fuente de donde provienen los datos.

---

[15] Base de datos que contiene el nombre, el tipo, el rango de valores, la fuente y la autorización para el acceso a cada elemento de los datos. Cuando la estructura de datos es considerada, también indica cuáles programas de la aplicación utilizan esos datos, de manera que se genere una lista de los programas afectados.

[16] Un elemento de datos es cualquier unidad de información definida para procesamiento.

b. Al 28 de mayo de 2010, la versión 2.2 del *Manual del Usuario, Nivel Operador del Sistema de Reservaciones (Manual del Usuario)*, que correspondía a la última revisión efectuada por el Desarrollador de Sistemas de Informática para la operación del *Sistema de Venta*, tenía las siguientes deficiencias:

1) En el *Manual del Usuario* no se incluía la siguiente información:

- La fecha de revisión y aprobación
- Un índice por temas y una descripción de la aplicación
- Un glosario para definir los términos principales utilizados en el sistema, tales como, punto de venta, concepto de venta, transacciones activas, transacciones históricas, reservaciones pilladas, excepción de crédito, extensiones y grupo activo
- Las instrucciones para acceder a las opciones de la pantalla *Mantenimiento* del menú *Grupos*, y a las opciones *Editar Pagos*, *Contratos*, *Excepciones de Crédito*, *Grupos* y *Cancelaciones* del menú *Transacciones*; *Clientes*, *Cuentas de Finanzas*, *Reservaciones Pilladas*, *Des_Bloquear Unidades*, *Bloquear Unidades*, *Des_Activar Recibos*, *Especiales* y *Seguridad* del menú *Mantenimiento*; y *Créditos*, *Reportes*, *Registro de Boletos*, *Consulta por Recibos* y *Reservaciones Por Cliente* del menú *Consultar* utilizadas por los usuarios del sistema
- Las instrucciones para aplicar los descuentos establecidos por ley; las tarifas y los descuentos promocionales; y los certificados de regalo (intercambios), a las transacciones que les correspondieran
- Las instrucciones para registrar en la pantalla *Otros Servicios* el cargo por concepto de los gastos administrativos ocurridos cuando un cliente requería un cambio de fecha, unidad o instalación

- Una lista de los mensajes de error producidos por el sistema y de los procedimientos que debía seguir el usuario para resolver estos errores
- Una lista de los informes producidos por el Sistema y sus usuarios. Además, no incluía procedimientos para la distribución del *Informe Diario Global*, *Informe Diario por Cajero*, *Informe Venta Boletos por Transacción* y el *Informe Venta Boletos por Usuario* que eran impresos por los usuarios e incluían información sobre los cuadres de transacciones diarias.

2) Las opciones de cuatro pantallas ilustradas en el *Manual del Usuario* no correspondían a las que presentaba el *Sistema de Ventas*.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el *Manual de Acceso*. En este se establece que la OSI será responsable de mantener periódicamente activos y actualizados los manuales operacionales de los sistemas de información y de sus aplicaciones, entre otros.

Además, son contrarias a lo establecido en la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular Núm. 77-05*. En esta se establece que toda aplicación comercial o personalizada implantada debe ser documentada mediante metodologías de desarrollo y documentación estándares o de uso común. Esta política se instrumenta, en parte, con el desarrollo y la actualización de la documentación de los sistemas y el establecimiento de un proceso uniforme para realizar y documentar los cambios a los sistemas. Este proceso debe incluir los pasos para asegurar que los cambios al sistema estén de acuerdo con las necesidades de la organización, y debidamente autorizados, documentados, probados y aprobados por la gerencia.

Las normas generalmente aceptadas en el campo de la tecnología de la información sugieren que las entidades deben mantener una documentación completa y actualizada de los sistemas en producción, así

como copias actualizadas y aseguradas fuera del área de sistemas de información. Una documentación adecuada del funcionamiento de un sistema computadorizado y sus programas provee información esencial para la implantación y la operación eficaz de este. Esta es de utilidad para el desarrollo de programas complementarios y es fuente de información para el estudio y la evaluación de los controles internos y para el adiestramiento del personal nuevo.

Efectos

Las situaciones comentadas en el **apartado a.** podrían ocasionar dificultades a los programadores, al personal de la OSI, a los usuarios y a los auditores para entender el funcionamiento de los procesos y de los controles de los tres sistemas de reservaciones y del contenido de su base de datos. Además, privan a la Compañía de información esencial para darle mantenimiento a dichos sistemas y dificulta mantener el control de los cambios a la programación y a la base de datos.

Las situaciones comentadas en el **apartado b.** podrían ocasionar que los usuarios utilizaran su propio criterio para realizar los trabajos asignados, lo que podría ocasionar falta de uniformidad para registrar las transacciones en el *Sistema de Ventas*. Además, propicia errores e irregularidades con los consiguientes efectos adversos en los procesos de reservaciones de la Compañía.

Causas

Las situaciones comentadas en el **apartado a.** se debían a que los exdirectores auxiliares de Sistemas de Información y la Ayudante Especial no habían requerido a los proveedores del *Sistema Reservaciones-Internet* y al Desarrollador de Sistemas de Informática que prepararan y mantuvieran actualizada la documentación de los sistemas de reservaciones utilizados por la Compañía.

Las situaciones comentadas en el **apartado b.** se debían, en parte, a que el Desarrollador de Sistemas de Informática no se había asegurado de que la información contenida en el *Manual del Usuario* estuviera completa y actualizada.

Comentarios de la Gerencia

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

> Según nuestra Oficina de Sistemas de Información, al momento no existe documentación alguna sobre el flujo de los procesos para las transacciones en línea. [*sic*] **[Apartado a.1)]**
>
> La Oficina de Sistemas de Información no cuenta con un Manual de Programador para sus aplicaciones. Se trabaja en la creación del mismo en colaboración con Consultores Externos. [*sic*] **[Apartado a.2)]**
>
> Según nuestro Desarrollador de Aplicaciones, no se documentan cambios hechos al sistema, sólo se hace una copia de la versión a la cual se le aplicarán los cambios luego de hacer pruebas. [*sic*] **[Apartado a.3)]**
>
> La Oficina de Sistemas de Información, indica que no existe manual para operador o guía técnica, sólo se utiliza el Manual de Usuario de la aplicación como referencia. Se proyecta desarrollar dicho manual en colaboración con los Consultores Externos. [*sic*] **[Apartado a.4)]**
>
> Según informa el Desarrollador de Aplicaciones, no existe un diccionario de datos para la aplicación de Reservaciones o para la base de datos, ya que por falta de personal y tiempo la aplicación aún continúa en desarrollo. [...] **[Apartado a.5)]**
>
> El Manual de Usuario para el Sistema de Ventas actualmente está en revisión [...]. Se proyecta someter el mismo al Director Ejecutivo y la Junta de Directores en o antes del 30 de junio de 2013. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1 y 3 de la d.5) a la e.

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 2 y 3** de este *Informe*. **[Hallazgos del 1 al 5]**

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

2. Ver que la Directora de Recursos Humanos, en coordinación con la Ayudante Especial, establezca un procedimiento para que se notifique a tiempo a la OSI el cese de un usuario en sus funciones. Este procedimiento debe incluir las medidas de control necesarias para desarrollar una comunicación efectiva entre la Oficina de Recursos Humanos y la OSI. Esto, para asegurar la pronta cancelación de las cuentas de acceso de estos usuarios. **[Hallazgo 1-a.1)]**

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

   a. Deshabilite, si aún no se ha realizado, las cuentas de acceso otorgadas a los empleados que hayan cesado sus funciones en la Compañía. Además, vea que, en lo sucesivo, las cuentas se deshabiliten en el momento en que el empleado cesa en sus funciones, de manera que no se repita la situación comentada en el **Hallazgo 1-a.1)**.

   b. Revise y actualice periódicamente los accesos otorgados al sistema *Reservaciones de Cabañas y Villas* y al *Sistema de Ventas*. Esto, para asegurarse de que los usuarios tengan asignados solamente los privilegios que necesitan para realizar las funciones relacionadas con los puestos que ocupan. **[Hallazgo 1-a.2)]**

   c. Establezca los controles necesarios para que se mantenga una segregación adecuada de las funciones conflictivas que realiza el Desarrollador de Sistemas de Informática. Además, se asegure de que en las situaciones extraordinarias en que se requiera a este empleado efectuar estas tareas, se establezcan controles alternos de supervisión y de revisión sobre las actividades que este realiza. **[Hallazgo 2-a.]**

d. Imparta instrucciones al Desarrollador de Sistemas de Informática para asegurarse de que:

1) Evalúe los niveles de acceso diseñados en la programación del *Sistema de Ventas* y en la base de datos *Reservaciones* para que se segreguen los accesos relacionados con la administración de la seguridad y con el registro de transacciones. **[Hallazgo 2-b.]**

2) Efectúe los cambios a la programación, si aún no se han realizado, para que se requiera a los usuarios del sistema *Reservaciones de Cabañas y Villas* y del *Sistema de Ventas* cambiar sus contraseñas cada 45 días, y utilizar contraseñas de más 7 caracteres que incluyan al menos un número, una letra y un carácter especial, según requerido en el *Manual de Acceso*. Una vez establecidos estos parámetros, se deberán impartir instrucciones a los usuarios para que efectúen el cambio de su contraseña. Esto, de manera que los nuevos parámetros de contraseña sean aplicados a todas las cuentas de usuario. **[Hallazgo 3-a.1) y 3)]**

3) Utilice un sistema de algoritmo seguro para encriptar y proteger las contraseñas de los usuarios almacenadas en la base de datos. **[Hallazgo 3-a.2)]**

4) Establezca medidas necesarias para que se mantenga la información sobre los usuarios que tienen o han tenido acceso a los sistemas de reservaciones. Esto, para poder acceder la información histórica de las transacciones generadas por estos usuarios y contenidas en la base de datos. **[Hallazgo 3-a.4)]**

5) Prepare y mantenga actualizada la documentación del *Sistema de Ventas*, del sistema *Reservaciones de Cabañas y Villas* y del *Sistema Reservaciones-Internet* para que incluya los diagramas de flujo sobre los procesos en línea; un manual del programador; evidencia de los

cambios efectuados a la programación y a la base de datos; un manual del operador; y un diccionario de datos. **[Hallazgo 5-a.]**

6) Revise el *Manual del Usuario* para asegurarse de que la información contenida en el mismo esté completa y actualizada. **[Hallazgo 5-b.]**

e. Una vez actualizado, refiera el *Manual del Usuario* para la aprobación del Director Ejecutivo y la Junta de Directores de la Compañía. **[Hallazgo 5-b.]**

f. Mantenga un registro, mediante un programa de administración de bases de datos, de los cambios efectuados a la información contenida en la base de datos *Reservaciones*, y refiera el mismo periódicamente a la Directora de la Oficina de Mercadeo y Servicio al Cliente para revisión. **[Hallazgo 4]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yermín M Valdivieso

ANEJO 1

COMPAÑÍA DE PARQUES NACIONALES DE PUERTO RICO

OFICINA DE SISTEMAS DE INFORMACIÓN

INFORME PUBLICADO

INFORME	FECHA	CONTENIDO DEL INFORME
TI-13-04	8 sep. 12	Controles internos para la administración del programa de seguridad, la continuidad del servicio, el acceso lógico y físico, y la red de comunicaciones de la Compañía.

ANEJO 2

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
Lcdo. Henry Neumann Zayas	Presidente	19 jun. 09	15 jul. 10
Ing. Jaime López	Director Ejecutivo de la Compañía de Turismo de Puerto Rico	19 jun. 09	15 jul. 10
Arq. Psj. Juan J. Terrasa Soler	Director Auxiliar Planificación de la Compañía de Turismo de Puerto Rico	19 jun. 09	15 jul. 10
Dr. Reinaldo del Valle Cruz	Ayudante Especial de la Secretaria del Departamento de Educación[17]	9 feb. 10	12 may. 10
Dr. Edward Moreno Alonso	Secretario Asociado del Departamento de Educación	19 jun. 09	17 dic. 09

[17] El Departamento de Educación no tuvo representación en la Junta de Directores durante los períodos del 18 de diciembre de 2009 al 8 de febrero de 2010 y del 13 de mayo al 15 de julio de 2010.

ANEJO 3

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
Sr. Daniel J. Galán Kercadó	Secretario de Recursos Naturales y Ambientales y Director Ejecutivo	19 jun. 09	15 jul. 10
Sra. Felícita Pizarro Calderón	Directora de Finanzas y Presupuesto	19 jun. 09	15 jul. 10
Sr. Carlos Calcador Díaz	Director de Administración	1 jul. 10	15 jul. 10
Sra. Yolanda Fonseca Torres	Directora de Administración	16 jul. 09	30 jun. 10
Sra. Clara Arriaga Correa	Directora Auxiliar de Administración[18]	19 jun. 09	15 jul. 09
Sra. Susan I. Peña De Jesús	Directora de Recursos Humanos[19]	19 jun. 09	30 jun. 10
Srta. Lymary Maymí Barreto	Ayudante Especial[20]	2 jul. 09	15 jul. 10
Sr. Daniel González Ruiz	Director Auxiliar de Sistemas de Información	19 jun. 09	15 jul. 10

[18] 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.

[19] El puesto de Directora de Recursos Humanos estuvo vacante del 1 de julio al 15 de julio de 2010. Durante dicho período las funciones del indicado puesto fueron ejercidas por la Sra. Felícita Pizarro Calderón, como Directora Interina.

[20] El puesto de Director de Sistemas de Información estuvo vacante del 19 de junio de 2009 al 15 de julio de 2010. Durante el período del 2 de julio de 2009 al 15 de julio 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