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

#859

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO SECRETARIA
SENADO DE P.R.
2013 AUG -1 AM 9:58

7 de marzo 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-13-16* de la Oficina de Sistemas de Información de la Administración de Corrección, adscrita al Departamento de Corrección y Rehabilitación, aprobado por esta Oficina el 22 de febrero de 2013. Publicaremos dicho *Informe* en nuestra página en Internet: http://www.ocpr.gov.pr para conocimiento de los medios de comunicación y de otras partes interesadas.

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

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

Cordialmente,

Yesmín M. Valdivieso

Anejo

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

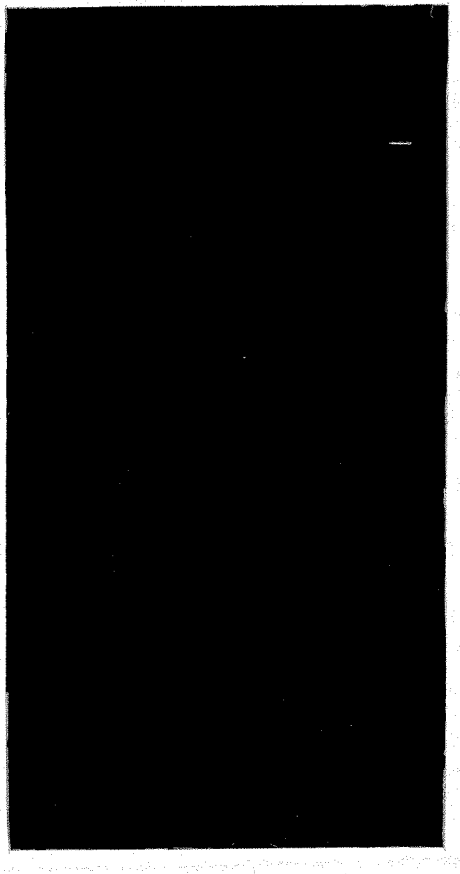
#859.

COMPROMISO • INTEGRIDAD
TRANSPARENCIA

SENSIBILIDAD • JUSTICIA • EXCELENCIA

[redacted]

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



INFORME DE AUDITORÍA TI-13-16

22 de febrero de 2013

Departamento de Corrección y Rehabilitación

Administración de Corrección

Oficina de Sistemas de Información

(Unidad 5001 - Auditoría 13479)

Período auditado: 2 de julio de 2010 al 29 de abril de 2011

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **4**

OPINIÓN Y HALLAZGOS **5**

1 - Uso de los servicios de Internet para fines ajenos a la gestión pública 5

2 - Información incompleta y no confiable en la base de datos del SCP, y falta de utilización de dicho sistema en varias instituciones de la Administración 8

3 - Falta de un plan de continuidad de negocios y de equipos para restaurar las operaciones en los centros alternos 13

4 - Deficiencias en el área donde estaban instalados los servidores, y en las áreas donde se encontraban los equipos computadorizados de dos instituciones 15

5 - Deficiencias relacionadas con los parámetros de seguridad configurados en el sistema operativo de seis servidores de la red 19

6 - Deficiencias relacionadas con el manejo y el almacenamiento de los respaldos de información 22

7 - Falta de inventarios físicos de la propiedad de los sistemas de información computadorizados y de un registro de programas instalados en cada computadora 25

8 - Falta de documentación del SCP 27

RECOMENDACIONES **28**

AGRADECIMIENTO **31**

ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **32**

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

22 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 Administración de Corrección (Administración), adscrita al Departamento de Corrección y Rehabilitación (Departamento), para determinar si las mismas 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 2 de julio de 2010 al 29 de abril de 2011. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene ocho hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, el acceso a los sistemas de información

computadorizados, la continuidad de servicio y el Sistema de Control de Población (SCP). Este *Informe* está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Administración se creó en virtud de la *Ley Núm. 116 del 22 de julio de 1974*, según enmendada. El *Plan de Reorganización Núm. 3* del 19 de diciembre de 1993, creó el Departamento y la Administración se adscribió y pasó a formar parte de este como un componente operacional.

La misión de la Administración es custodiar y proveer los servicios a los confinados para rehabilitarlos e integrarlos a la libre comunidad. Su visión es desarrollar de manera efectiva los programas de tratamiento y desvío para maximizar la rehabilitación y estabilizar los niveles de población en las instituciones penales, a través de una estructura administrativa eficiente que permita la reorganización y el uso de la mejor tecnología.

La Administración es dirigida por un Administrador, quien, a su vez, es el Secretario de Corrección y Rehabilitación (Secretario). Este es nombrado por el Gobernador con el consejo y consentimiento del Senado.

A la fecha de nuestra auditoría, la OSI contaba con un Especialista en Sistemas de Información, quien realizaba las funciones de Director; cuatro técnicos de reparación de equipo electrónico; dos analistas programadores y dos oficinistas. Además, la Administración tenía contratada una compañía, la cual proveía servicios de asesoría en sistemas de información, entre otros: análisis y desarrollo de aplicaciones, y administración de bases de datos y de red de comunicaciones.

La Administración tiene dos aplicaciones principales: el SCP y el Sistema Electrónico de Recopilación de Totales Automatizado (Sistema Serta). En el SCP se mantenía una base de datos con la información de los confinados, tal como: fotos, huellas, localización, sentencias, delitos y nivel de custodia. El Sistema Serta se utiliza para registrar los datos del conteo diario de la población penal de cada institución para conocer el

estado de cumplimiento de las instituciones con las capacidades establecidas y aprobadas por el Tribunal Federal (*Morales Feliciano* v. *Romero Barceló*, 497 F. Supp. 14, 32, PR 1979).

El presupuesto de la Administración proviene de resoluciones conjuntas del Fondo General del Estado Libre Asociado de Puerto Rico, de asignaciones especiales del Fondo Presupuestario, de fondos federales para gastos de funcionamiento, de asignaciones legislativas y federales para mejoras permanentes, y de préstamos y emisiones de bonos. Para los años fiscales del 2008-09 al 2010-11, el presupuesto de la Administración ascendió a $402,953,000, $337,727,000 y $339,618,000.

Mediante el *Plan de Reorganización Núm. 2* del 21 de noviembre de 2011 se derogó la *Ley Núm. 116* y se transfieren al Departamento los empleados y funcionarios, expedientes, equipos, materiales, fondos y asignaciones, entre otros, de la Administración.

El **ANEJO** contiene una relación de los funcionarios principales del Departamento y de la Administración que actuaron durante el período auditado.

La Administración cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.ac.gobierno.pr. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas por nuestros auditores mediante cartas del 18 y 31 de mayo de 2011 al Hon. Carlos M. Molina Rodríguez, Secretario de Corrección y Rehabilitación, y Administrador de Corrección durante el período auditado. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 3 y 9 de junio de 2011, el Sr. Edgardo Centeno Soto, Secretario Auxiliar de Auditoría Interna y el Sr. Ángel Batiz Rodríguez, Funcionario Enlace del Secretario en Sistemas de Información, durante

el período auditado, remitieron sus comentarios sobre los **hallazgos** incluidos en las cartas de nuestros auditores. Dichos comentarios fueron considerados en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Lcdo. Jesús González Cruz, entonces Secretario de Corrección y Rehabilitación, por carta del 23 de octubre de 2012 y al señor Molina Rodríguez, ex Secretario de Corrección y Rehabilitación, por carta del 30 de octubre de 2012. En este se indicaron datos específicos, tales como: nombres, cuentas de acceso y localizaciones, que por seguridad no se incluyen en este *Informe*.

El entonces Secretario de Corrección y Rehabilitación contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 7 de diciembre de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*. En los **hallazgos** se incluyeron algunos de sus comentarios.

Mediante carta del 26 de noviembre 2012, se le dio seguimiento a la carta del 30 de octubre de 2012 que se le envió al ex-Secretario con el borrador de los **hallazgos** de este *Informe*. No obstante, este no contestó.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas revelaron que las operaciones de la OSI, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, el acceso a los sistemas de información computadorizados, la continuidad de servicio y el SCP, no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 8** que se comentan a continuación.

Hallazgo 1 - Uso de los servicios de Internet para fines ajenos a la gestión pública

Situación

a. La Administración mantiene un servidor que permite acceso a Internet a los usuarios autorizados. Dicho servidor produce diariamente un archivo en el cual se registran todas las direcciones de las páginas de Internet que son accedidas por las cuentas de los usuarios.

El examen del registro de direcciones de Internet visitadas por los usuarios de la Administración el 27 de agosto de 2010, reveló que ese día se utilizó este servicio para acceder 166 páginas en Internet con contenido ajeno a la gestión pública. No se pudieron identificar las cuentas de acceso de los usuarios que visitaron las mismas, porque el servidor no estaba configurado para que se registrara el nombre del usuario que accedía a las páginas en Internet.

Criterios

La situación comentada es contraria al Artículo VI, Sección 9 de la Constitución y al Artículo 3.2(c) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*[1], según enmendada. También es contraria a los artículos VI y VII del *Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas de Información*, según enmendado, aprobado el 15 de noviembre de 2006 por el Secretario de Corrección y Rehabilitación.

Efectos

La situación comentada desvirtúa los fines públicos para los cuales se adquirieron las computadoras. Además, provee al funcionario o empleado que indebidamente las utiliza, ventajas, beneficios y privilegios que no están permitidos por ley.

Por otro lado, el acceso a páginas en Internet y a mensajes de correo electrónico ajenos al fin público expone a los equipos y a la información sensitiva almacenada en los sistemas, a riesgos innecesarios como son la

[1] Esta *Ley* fue derogada por la *Ley 1-2012, Ley de Ética Gubernamental de Puerto Rico de 2011*, la cual en el Artículo 4.2 (b) contiene disposiciones similares.

propagación de virus, *spyware*[2], *phishing*[3], *spoofing*[4], *spamming*[5] y ataques de negación de servicios[6], entre otros, que pudieran afectar la continuidad de las operaciones de la Administración, sin que se puedan fijar responsabilidades.

Causas

Las situaciones comentadas se debían, en parte, a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso y el manejo de las cuentas para acceder a Internet
- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento de los usuarios con las normas establecidas sobre el uso oficial de las cuentas para acceder a Internet.

Comentarios de la Gerencia

En la carta del entonces Secretario de Corrección y Rehabilitación, este nos indicó, entre otras cosas, lo siguiente:

> El sistema de acceso al Internet de la Administración de Corrección está estructurado según lo establecen las mejores prácticas de la industria [...]. La AC utiliza la herramienta de [...], provista por la Oficina de Gerencia y Presupuesto. [*sic*]

---

[2] Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

[3] Es un tipo de ataque de correo electrónico que trata de convencer a un usuario de que el originador es auténtico, pero con la intención de obtener información.

[4] Es un ataque activo en el que el intruso presenta una identidad que no es la identidad original. En este ataque el propósito es obtener acceso a los datos sensitivos o a los recursos de los sistemas de información computadorizados a los que no se permite el acceso bajo la identidad original.

[5] Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

[6] Ocurren cuando una computadora conectada a Internet es inundada con datos y solicitudes que deben ser atendidas. La máquina se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades.

> [...] estaremos redefiniendo los accesos a todos los usuarios en una campaña que denominaremos Ponte tu Sistema al Día. En esta estaremos orientando a los usuarios sobre el uso de los sistemas y sus políticas, incluyendo el acceso a internet. [*sic*]

Véase la Recomendación 1.a. y b.

Hallazgo 2 - Información incompleta y no confiable en la base de datos del SCP, y falta de utilización de dicho sistema en varias instituciones de la Administración

Situaciones

a. Desde enero de 2004, la Administración tiene en funcionamiento el SCP para mantener el control de la custodia de las personas convictas y confinadas en las instituciones y los complejos correccionales. Dicho sistema mantiene una base de datos con la información descriptiva de los confinados, tal como: fotos, huellas digitales, localización, sentencias, delitos y nivel de custodia. El SCP fue desarrollado e implantado por una compañía mediante contratos de servicios profesionales en el área de sistemas de información desde el 1 de febrero de 2003 hasta el 30 de junio de 2009[7] por $10,430,563.

   En los centros de ingreso de la Administración[8] se realiza la entrada de datos inicial para la creación del registro del confinado en el SCP. Luego, en las instituciones se registra la información relacionada con la ubicación del confinado y las evaluaciones realizadas por los trabajadores sociales de cada unidad. Una vez el confinado recibe sentencia del tribunal, se registra la información de la misma en el SCP.

   La tabla *admision* de la base de datos del SCP contenía 194,184 registros. En esta se mantenía la información que fue registrada por el Técnico de Mesa durante el proceso de admisión del confinado al sistema correccional.

---

[7] El 1 de julio de 2009 la Administración otorgó un contrato a otra compañía para proveer los servicios técnicos para asegurar la continuidad de la operación del sistema, y apoyo a los usuarios.

[8] Los centros de ingresos son: la Escuela Industrial de Mujeres de Vega Alta, el Centro de Ingresos Metropolitano de Bayamón (705), el Centro de Ingresos del Sur (Ponce 676) y la Institución Correccional Guerrero en Aguadilla.

La tabla *record_confinados* de la base de datos del SCP contenía 43,396 registros de confinados activos[9]. En dicha tabla se mantenía toda la información del confinado relacionada con los delitos, las sentencias, la institución asignada y la fecha de ingreso, entre otra.

1) El examen efectuado el 16 de febrero de 2011 para determinar la integridad de la información contenida en la tabla *admision* y los controles para la validación de los datos establecidos para registrar esta información, reveló las siguientes deficiencias:

a) No se incluyó la siguiente información en la tabla *admision*:

INFORMACIÓN DEL CONFINADO NO REGISTRADA	CANTIDAD DE REGISTROS
Fecha de nacimiento	52,377
Descripción de la constitución física	41,141
Estatura	40,223
Color de cabello	39,506
Color de ojos	39,846
Peso	39,759
Número[10]	38,318
Status[11]	35,101
Número de seguro social federal	11,131
Nombre	524
Primer apellido	518
Fecha de admisión	384
Número de admisión[12]	317

[9] El campo *DCR Status* identificaba si la Administración tenía custodia del confinado (Activo), ya fuera que estuviera encarcelado o en libertad condicionada, o si ya el confinado había cumplido su sentencia (Inactivo). Los registros activos se refieren a aquellos que indicaban en el campo *DCR Status* la palabra Activo.

[10] El número de confinado es el que identifica el registro del confinado en el SCP. Dicho número es asignado por la Oficina de Récord y Documentos.

[11] El *status* del confinado debía ser sumariado o sentenciado.

[12] Este número lo genera el SCP una vez se termina el proceso de admisión del confinado.

b) En 36 registros de confinados se indicaba que las edades de estos fluctuaban de 0 a 10 años. Además, en 46 registros se indicaba que las edades de los confinados fluctuaban de -1 a -426.

c) En 371 registros de confinados se indicaba que el peso de estos fluctuaba entre 0 y 40 libras.

d) En 359 registros de confinados se indicaban estaturas que fluctuaban desde .49 a 2.95 pies. Además, en 15 registros se indicaban estaturas que fluctuaban entre 8 y 9.8 pies. En 18 registros se incluyó un punto en dicho campo.

e) En el campo que identificaba el color de ojos se indicaban descripciones, tales como: Azulejos, B, Claros, Geisel, Grisoso, H, Heisel, Heizel, Largos, Multicolor, Otros, Rosa y Se Desconoce.

f) En el campo que identificaba la fecha de admisión encontramos las siguientes fechas: 2-Nov-1848, 1-Jan-1900, 2-Jan-1900, 11-Sep-2011, 23-May-2013, 15-Jan-2019, 17-Jun-2030, 9-Aug-2050, 8-Sep-2050, 28-Dec-2050, 10-Feb-2060, 4-Apr-2065, 12-Feb-2070, 20-Feb-2070, 2-Mar-2070, 13-Feb-2080, 6-Nov-2080, 16-Nov-2080, 1-Jun-2090, 25-Nov-2097 y 16-Apr-2099.

g) En 50,522 registros no se incluyó el nombre del agente del orden público que custodiaba al confinado al momento de la entrada al centro de ingreso.

h) En 50,948 registros no se incluyó el número de placa del agente de orden público que custodiaba al confinado al momento de la entrada al centro de ingreso.

2) El examen efectuado el 16 de febrero de 2011 para determinar la integridad de la información contenida en la tabla *record_confinados*, y los controles para la validación de los datos establecidos para registrar esta información, reveló las siguientes deficiencias:

a) En el campo *Jail status* en el que se indicaba si el confinado estaba encarcelado (Activo) o en libertad condicionada (Inactivo), se identificaron 1,753 registros en los que se incluyó la palabra Tinactivo. El personal de la OSI no nos pudo explicar el significado de este término.

b) La tabla *record_confinados* de la base de datos del SCP contenía 5,402 registros de confinados con un nivel de seguridad máxima en el campo *nivel_seguridad*. De estos, 1,329 registros indicaban Inactivo en el campo *Jail status*, lo que no corresponde al nivel de seguridad máxima que requieren estos confinados.

c) En 22,160 registros de confinados no se les había establecido el nivel de seguridad. A los confinados se les debía establecer uno de tres niveles de seguridad disponibles: mínima, mediana o máxima.

d) En el campo *date-in* se registraba la fecha de ingreso del confinado al sistema correccional. Se encontró que la fecha de ingreso más antigua que mostraba el SCP era el 1 de octubre de 2003, aun cuando en el sistema correccional hay confinados que ingresaron antes de esa fecha.

b. Al 13 de abril de 2011, había ocho instituciones en las cuales el SCP estaba inoperante, por lo que la información de los confinados ubicados en las mismas no estaba registrada en dicho Sistema. Las instituciones eran las siguientes:

- Institución Correccional Zarzal
- Hogar de Adaptación Social de Fajardo

- Hogar Intermedio para Mujeres
- Centro de Tratamiento Residencial de Humacao
- Hospital Psiquiátrico Correccional
- Centro con Libertad para Trabajar de Ponce
- Centro de Tratamiento Residencial de Arecibo
- Hogar de Adaptación Social de Mayagüez

Criterio

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 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. Esta política se instrumenta mediante sistemas computadorizados que cuenten con los controles necesarios que permitan asegurar la integridad de la información contenida en la base de datos del SCP, y garantizar la accesibilidad a información completa y confiable.

Efectos

Las situaciones comentadas afectan la integridad y la confiabilidad de la información de los confinados que se mantiene en el SCP, y pueden dar lugar a la comisión de errores e irregularidades, sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas. Además, podrían afectar el control que se debe mantener sobre la población correccional.

Causas

Las situaciones comentadas en el **apartado a.** se debían, en parte, a lo siguiente:

- El SCP no validaba la información registrada en dichos campos e incluso permitía dejarlos en blanco.

- Los técnicos de récord en las instituciones no cumplían con sus responsabilidades al registrar la información relacionada con los confinados.
- No había un manual de usuario para los procedimientos de control de entrada de datos al SCP.

La situación comentada en el **apartado b.** se debía a fallas eléctricas, servidores averiados o problemas de conexión a la red en dichas instituciones.

Comentarios de la Gerencia

En la carta del entonces Secretario de Corrección y Rehabilitación, este nos indicó, entre otras cosas, lo siguiente:

> El Sistema de Control de Población fue desarrollado durante los pasados años. Su arquitectura es una abierta permitiendo la entrada libre de datos en todos los campos del sistema. Esta apertura del sistema evita que se puedan validar los campos de la aplicación permitiendo la entrada libre de información. [*sic*] **[Apartado a.]**
>
> Debido a la cantidad de las localizaciones donde se encuentra el sistema y su peculiaridad de trabajar por separado en cada localización, las diferentes localidades en un momento dado pueden tener problemas y no funcionar adecuadamente. Las situaciones en los distintos complejos varían constantemente y muchas no dependen de la OSI, no obstante se trabaja con las otras oficinas del departamento para atender cualquier situación que surja. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1.c. y d., y 2.

Hallazgo 3 - Falta de un plan de continuidad de negocios y de equipos para restaurar las operaciones en los centros alternos

Situaciones

a. La Administración 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. La OSI había identificado dos instituciones como centros alternos para restaurar las operaciones computadorizadas, en caso de que alguna emergencia impidiera utilizar los equipos de comunicación de la Administración. De acuerdo con la información provista por el personal de la OSI, en estas instituciones había unos servidores adicionales para ser utilizados en caso de que surgiera una emergencia. Sin embargo, en visitas realizadas el 20 de enero y el 9 de febrero de 2011, nuestros auditores y el personal de estas instituciones no identificaron los servidores adicionales que debían ser utilizados para asegurar la continuidad de las operaciones en caso de emergencia. El 23 de marzo de 2011 el Especialista en Sistemas de Información nos proveyó una certificación que indicaba que los servidores adicionales se encontraban en la OSI.

Criterios

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

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

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

Efectos

La situación comentada en el **apartado a.** podría propiciar la improvisación y, que en casos de emergencia, se tomen medidas

inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos y de interrupciones prolongadas de las operaciones de la Administración.

La situación comentada en el **apartado b.** podría afectar las funciones de la Administración y los servicios de la OSI, ya que no tendrían disponible en las instalaciones seleccionadas como centro alterno, el equipo necesario para restaurar sus archivos y sistemas, y restablecer prontamente sus operaciones normales.

Causas

La situación comentada en el **apartado a.** se atribuye a que el Secretario de Corrección y Rehabilitación en funciones no le había requerido al Especialista en Sistemas de Información que preparara un plan de continuidad de negocios para los sistemas de información, que proveyera las estrategias para responder ante cualquier desastre.

La situación comentada en el **apartado b.** se atribuye a que el Especialista en Sistemas de Información no se había asegurado de mantener los servidores requeridos en las instituciones identificadas como centros alternos, para ser utilizados en caso de que alguna situación inusual o de emergencia impidiera utilizar los servidores instalados en el edificio principal de la Administración.

Véanse las recomendaciones 1.e. y 3.

Hallazgo 4 - Deficiencias en el área donde estaban instalados los servidores, y en las áreas donde se encontraban los equipos computadorizados de dos instituciones

Situaciones

a. La Administración tenía ubicados los servidores principales, el *switch*[13] principal y la unidad para realizar los respaldos en un área

[13] Dispositivo de comunicación central que conecta dos o más segmentos de red y permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

designada dentro del centro de cómputos del Departamento de Educación. El examen efectuado al área donde estaban instalados dichos equipos reveló lo siguiente:

1) El área no cumplía con las condiciones ambientales adecuadas para proteger los equipos de sistemas de información. En esta observamos materiales inflamables, tales como: cajas de cartón, plástico y pedazos de paneles acústicos de techo.

2) No había un diagrama esquemático de la infraestructura de la red en un lugar visible, y los cables utilizados para las conexiones entre los equipos computadorizados y de comunicaciones (cableado) no estaban identificados, organizados ni amarrados. Esto era necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones.

3) Los siguientes equipos, que pertenecían a la Administración, no estaban identificados con número de propiedad:

DESCRIPCIÓN	CANTIDAD
Switch DELL 3348 48 ports	2
CISCO router 2600	2
Batería *Valere Power*	2
CISCO router 3700	1
ProCurve Switch 1700-8	1
Switch Catalyst 4506	1
Router Centennial	1
Batería *MinuteMan E3200*	1

b. El examen realizado al área donde se encontraban los equipos computadorizados del Centro de Ingresos Metropolitano de Bayamón, reveló las siguientes deficiencias:

1) El área donde estaba el gabinete de cableado (*wiring closet*) no cumplía con las condiciones ambientales adecuadas para proteger los equipos de sistemas de información. En esta observamos materiales inflamables, tales como: planos y documentos en cajas de cartón.

2) El cableado no estaba identificado ni organizado.

3) Los equipos computadorizados no estaban identificados con número de propiedad.

c. El examen efectuado al área donde se encontraban los equipos computadorizados del Centro de Ingresos del Sur, reveló lo siguiente:

1) No había un diagrama esquemático de la infraestructura de la red en un lugar visible y el cableado no estaba identificado.

2) El área donde estaba el gabinete de cableado (*wiring closet*) no cumplía con las condiciones ambientales adecuadas para proteger los equipos de sistemas de información. En dicha área, junto al gabinete, había una nevera pequeña, una tostadora y una cafetera.

3) Los siguientes equipos no estaban identificados con número de propiedad:

DESCRIPCIÓN	CANTIDAD
Servidor *DELL Power Edge 2850*	2
Batería *MinuteMan Enterprise E3200*	2
Teclado *DELL*	2
Mouse *DELL*	2
Omni Switch 6648 de 48 puertos	1
DELL Power Connect 3348 de 48 puertos	1
Monitor *DELL*	1
DELL PowerVault 122T DLT VS-80	1
Disco Externo *Omega* de 1 terabyte	1

Situaciones similares a las comentadas en los **apartados a.3), b.3) y c.3)** fueron comentadas en el *Informe de Auditoría TI-99-8* del 25 de mayo de 1999.

Criterios

Las situaciones comentadas en los **apartados a.3), b.3) y c.3)** se apartan a lo establecido en la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, y en el

Artículo XI del *Reglamento 11, Normas Básicas para el Control y la Contabilidad de los Activos Fijos*, aprobado el 29 de diciembre de 2005 por el Secretario de Hacienda.

Las situaciones comentadas en los **apartados a.1) y 2), b.1) y 2) y c.1) y 2)** son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Efectos

Las situaciones comentadas en los **apartados a.1), b.1) y c.2)** pueden propiciar daños a las instalaciones y a los equipos, y provocar eventos de interrupción de servicios. Esto puede afectar la continuidad de las operaciones de los sistemas de información computadorizados de la Administración.

Las situaciones comentadas en los **apartados a.2), b.2) y c.1)** impiden a la Administración obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificultan la atención de problemas de conexión en un tiempo razonable, y planificar eficazmente las mejoras a la red según el crecimiento de sus sistemas.

Las situaciones comentadas en los **apartados a.3), b.3) y c.3)** impiden mantener un control adecuado de la propiedad y pueden propiciar el uso indebido o la pérdida de la misma, sin que se puedan detectar a tiempo para fijar responsabilidades. Además, dificultan la identificación y la localización de los equipos. También dificultan nuestra gestión fiscalizadora.

Causas

Las situaciones comentadas en los **apartados a.1), b.1) y c.2)** se atribuyen a que el Especialista en Sistemas de Información no se aseguró de mantener las condiciones ambientales adecuadas que minimicen el riesgo de daños a los equipos computadorizados.

Las situaciones comentadas en los **apartados a.2), b.2) y c.1)** se atribuyen a que el Especialista en Sistemas de Información no había impartido

instrucciones para que se mantuvieran los diagramas esquemáticos visibles, y para que el cableado estuviera identificado, organizado y amarrado.

Las situaciones comentadas en los **apartados a.3), b.3) y c.3)** se atribuyen a que la Encargada de la Propiedad no cumplió con su responsabilidad de numerar y marcar todos los equipos de la Administración.

Comentarios de la Gerencia

En la carta del entonces Secretario de Corrección y Rehabilitación, este nos indicó, entre otras cosas, lo siguiente:

> [...] al momento las facilidades de Educación proveen todos los elementos necesarios que requieren un centro de cómputos. [*sic*]
>
> Las facilidades en las instituciones antes mencionados han sido revisadas para cumplir con los requerimientos básico necesarios y según nuestro análisis estas cumplen con los criterios básicos necesarios para el tipo de importancia y servicio que ofrecen estas localidades. [*sic*]

Véanse las recomendaciones 1 de la f. a la h., 4 y 5.

Hallazgo 5 - Deficiencias relacionadas con los parámetros de seguridad configurados en el sistema operativo de seis servidores de la red

Situaciones

a. La Administración tenía 35 servidores. El examen efectuado sobre los parámetros de control de acceso y de seguridad definidos en el sistema operativo de seis servidores reveló las siguientes deficiencias en la utilización de las opciones que permiten controlar la seguridad de las cuentas de los usuarios:

   1) En los seis servidores no se habían activado los parámetros para:

      a) Requerir, al menos, ocho caracteres para la utilización de las contraseñas (*Minimum Password Length*) conforme se establecía en la reglamentación interna de la Administración. Las contraseñas estaban definidas para permitir, por lo menos, cinco caracteres.

b) Requerir, al menos, cinco contraseñas diferentes antes de volver a utilizar la misma (*Enforce Password History*).

c) Requerir que las contraseñas utilizadas fueran combinaciones alfanuméricas (*Password must meet complexity requirements*).

d) Definir un término de inactividad, de al menos 15 minutos, para que luego el sistema requiriera una contraseña para continuar con el uso del mismo (*Account Lockout Duration*).

e) Definir un término, de al menos tres intentos de acceso sin éxito, para que el sistema deshabilitara la cuenta (*Account Lockout Threshold*).

2) El examen efectuado a la configuración de las políticas de auditoría (*Audit Policy*), los privilegios de los usuarios (*User Rights Assignment*) y las opciones de seguridad (*Security Options*) establecidas en los servidores examinados, reveló que no se habían establecido los parámetros de acuerdo con las recomendaciones incluidas en las guías de seguridad publicadas por el proveedor, según se indica:

a) No se había definido la política de auditoría (*Audit Policy*) para que el sistema produjera un registro cuando ocurriera lo siguiente:

- Los eventos de acceso de las cuentas (*Audit Account Logon Events*) y los eventos de acceso (*Audit Logon Events*)

- La creación, modificación o eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit Account Management*)

- Los accesos a los archivos, cartapacios (*folders*) e impresoras (*Audit Object Access*)
- Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit Policy Change*)
- El uso de los privilegios de los usuarios (*Audit Privilege Use*)
- El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit System Events*).

b) No se habían definido las opciones para activar o desactivar los siguientes parámetros de seguridad:

- *Shutdown system immediately if unable to log security audits*
- *Allow undock without having to log on*
- *Require strong session key*
- *Display user information when the session is locked*
- *Require Domain Controller authentication to unlock workstation*
- *Do not allow storage of credentials or.NET Passports for network authentication*
- *Do not store LAN Manager hash value on next password change*
- *Force strong key protection for user keys stored on the computer*
- *Default owner for objects created by members of the Administrators Group*
- *Use Certificate Rules on Windows Executable for Software Restriction Policies.*

Criterios

Estas situaciones se apartan de lo establecido en el *Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas de Información* y en las políticas *TIG-003* y *TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la *Carta Circular 77-05*.

Efectos

La situación comentada en el **apartado a.1)** propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **apartado a.2)** impide a la Administración mantener un registro de los eventos inusuales o los problemas ocurridos en la red que le permitiera al personal de la OSI tomar a tiempo las medidas correctivas o preventivas necesarias.

Causa

Las situaciones comentadas se debían a que el Especialista en Sistemas de Información no se aseguró de que el personal encargado de administrar los sistemas pusiera en vigor todas las opciones de seguridad de acceso lógico que proveen los sistemas operativos.

Véase la Recomendación 1.i. y j.

Hallazgo 6 - Deficiencias relacionadas con el manejo y el almacenamiento de los respaldos de información

Situaciones

a. La Administración había establecido una *Estrategia de Resguardo y Recuperación de Datos (Manual DCR-2009-02)* aprobada el 13 de noviembre de 2009 por el Secretario de Corrección y Rehabilitación. En este *Manual* se establecía, entre otras cosas, que se realizarán respaldos diarios diferenciales (*differentials backups*) y respaldos completos semanales (*full backups*). Se establecía, además,

que se realizaría una rotación cíclica de cintas de respaldos. Según el *Manual*, la rotación cíclica semanal utilizaba 3 *sets* de cintas, cada *set* contiene 14 unidades de cintas *LTO Ultrium 400 GB* (2 por día). Mientras transcurre una semana 1 *set* de cintas permanece dentro de la librería y los otros 2 *sets* se quedan en un lugar remoto al edificio[14]. Los respaldos de información eran realizados por un técnico de una compañía contratada para ofrecer servicios profesionales de sistemas de información. El último respaldo semanal del mes era el que se enviaba al centro de respaldo alterno. El primer lunes de cada mes se enviaba al centro de respaldo alterno el *set* de cintas de respaldo de la última semana del mes anterior.

En el examen realizado sobre el proceso de manejo y almacenamiento de los respaldos de información determinamos lo siguiente:

1) No se realizaba, según se establecía en el *Manual DCR-2009-02*, la rotación cíclica semanal de las cintas de respaldos. El mismo *set* de cintas permanecía en la librería, ubicada en el centro de cómputos, durante todo el mes.

2) Al 16 de febrero de 2011, las cintas con los respaldos mensuales de noviembre y diciembre de 2010, y de enero de 2011, no habían sido enviadas al centro de respaldo alterno. Estas cintas permanecieron en el centro de cómputos donde estaban localizados los servidores de la Administración.

3) En la OSI no se mantenía un registro de los respaldos realizados ni de las cintas enviadas al centro de respaldo alterno, en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor donde se mantenían estos archivos, la última fecha de actualización de la información y la explicación de fallas o situaciones especiales que ocurrieron, si alguna, durante la preparación de los respaldos.

---

[14] En el *Manual* no se identificó el lugar.

4) Las cintas de los respaldos enviados al centro de respaldo alterno no estaban identificadas con el contenido de la cinta y la fecha del respaldo, y no estaban protegidas contra el agua. El sistema de supresión de incendios del área donde se guardaban las cintas de respaldos era de rociadores de agua.

Situaciones similares a las indicadas en el **apartado a.3) y 4)** fueron comentadas en el *Informe de Auditoría TI-99-8*.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el *Manual DCR-2009-02* y en la *Política TIG-003* de la *Carta Circular 77-05*. Conforme con dicha política pública, se requiere mantener una copia de los respaldos almacenada en un lugar seguro fuera del edificio donde está instalada la computadora principal y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias. Por otro lado, se debe mantener un inventario detallado de los medios magnéticos de respaldos para facilitar su localización y para sustituir periódicamente, por medios magnéticos nuevos, los utilizados para los respaldos.

Efectos

Las situaciones comentadas en el **apartado a.1) y 2)** pueden ocasionar que, en casos de emergencias, la Administración no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Las situaciones comentadas en el **apartado a.3) y 4)** dificultan la localización y la identificación del contenido de las cintas de respaldos, lo que podría afectar el proceso de restauración de los sistemas afectados en caso de contingencias o emergencias.

Causas

La situación comentada en el **apartado a.1)** se debía, en parte, a que el Especialista en Sistemas de Información no tomó las debidas precauciones para asegurarse de que el técnico de una compañía contratada para ofrecer servicios profesionales de sistemas de información, encargado de realizar

los respaldos, cumpliera con lo establecido en el *Manual*. Tampoco se aseguró de que el personal de la OSI enviara las cintas de los respaldos al centro alterno de recuperación. **[Apartado a.2)]**

Las situaciones comentadas en el **apartado a.3) y 4)** se debían, en parte, a que en el *Manual* no se incluyeron los requisitos de mantener un registro de los respaldos ni la identificación de los mismos.

Véase la Recomendación 1 de la k. a la m.

Hallazgo 7 - Falta de inventarios físicos de la propiedad de los sistemas de información computadorizados y de un registro de programas instalados en cada computadora

Situaciones

a. Al 7 de marzo de 2011, la Encargada de la Propiedad de la Administración no tenía un inventario de los equipos computadorizados que incluyera, entre otras cosas, la descripción, el número de propiedad, la fecha de adquisición, el precio unitario y la localización.

b. Al 1 de noviembre de 2010, la OSI no contaba con un registro de los programas adquiridos e instalados en las computadoras que incluyera, entre otras cosas, el número de la licencia del programa, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado y el total de licencias adquiridas.

Criterios

Estas situaciones se apartan de lo establecido en la *Ley Núm. 230*, en el *Reglamento 11*, en el *Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas de Información* y en la *Política TIG-008* de la *Carta Circular 77-05*.

Efectos

La situación comentada en el **apartado a.** impide a la Encargada de la Propiedad mantener un control adecuado de los equipos computadorizados

bajo su custodia. Además, propicia el ambiente para el uso indebido o la desaparición de los mismos y otras situaciones adversas, sin que se puedan detectar a tiempo para fijar responsabilidades.

La situación comentada en el **apartado b.** impide ejercer un control eficaz de los programas y las licencias correspondientes. Además, propicia la 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 Administración. También limitó el alcance de nuestro examen sobre los programas instalados en las computadoras examinadas.

Causas

La situación comentada en el **apartado a.** se debe a que la Encargada de la Propiedad no cumplió con su responsabilidad de mantener un inventario de la propiedad de la agencia.

La situación comentada en el **apartado b.** se debe a que el personal de la OSI no cumplió con lo establecido en el *Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas de Información.*

Comentarios de la Gerencia

En la carta del entonces Secretario de Corrección y Rehabilitación, este nos indicó, entre otras cosas, lo siguiente:

> La OSI tiene un inventario de los equipos y los programas instalados. A continuación hemos incluido dicho listado. [...]

Consideramos las alegaciones del entonces Secretario, pero determinamos que el **Hallazgo** prevalece, porque el inventario incluido con sus comentarios no contiene la información necesaria para mantener el control de los equipos y los programas computadorizados.

Véanse las recomendaciones 1.n. y 5.

Hallazgo 8 - Falta de documentación del SCP

Situaciones

a. El examen realizado a la documentación del SCP reveló lo siguiente:

1) La Administración no contaba con documentación que incluyera, entre otras cosas, el lenguaje de la programación, la fecha de creación, y el equipo y el sistema operativo utilizado para operar el SCP.

2) La Administración no contaba con un manual de usuario del SCP, que incluyera, entre otras cosas, lo siguiente:

- La descripción de la aplicación
- La descripción de los documentos que originan las transacciones
- Las instrucciones para preparar los documentos que originan las transacciones
- Las instrucciones para realizar los distintos procedimientos disponibles en el sistema
- Los procedimientos de control en cuanto a la segregación de deberes, la supervisión del personal y la autorización de las transacciones
- El procedimiento para identificar y corregir errores
- La descripción de los informes y de los usuarios de estos
- La frecuencia de reproducción y distribución de los informes.

Criterios

La situación comentada es contraria a lo establecido en la *Política TIG-011* de la *Carta Circular 77-05*. Esta política se instrumenta, en parte, mediante el desarrollo y la actualización de la documentación de los sistemas.

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

Efecto

La situación comentada dificulta el entendimiento del funcionamiento del SCP por parte de los programadores, de los usuarios y de los auditores que evalúan el mismo.

Causas

La situación comentada se debía a que el Secretario de Corrección y Rehabilitación no se aseguró de que se incluyeran cláusulas en los contratos otorgados a la compañía que desarrolló el SCP para que se le requiriera la documentación indicada.

Véase la Recomendación 6.

RECOMENDACIONES

Al Secretario de Corrección y Rehabilitación

1. Ejercer una supervisión efectiva sobre el Director de Sistemas de Información para asegurarse de que:

    a. Oriente a los usuarios de los sistemas de información sobre las disposiciones del *Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas de Información* para asegurarse de que estos cumplan con las normas establecidas sobre el uso oficial de las cuentas para acceder a Internet. **[Hallazgo 1]**

b. Realice inspecciones periódicas para asegurarse de que los usuarios cumplan con las normas establecidas sobre el uso oficial de las cuentas para acceder a Internet. **[Hallazgo 1]**

c. Establezca las medidas de control necesarias para que se valide la información al momento de registrarla en el SCP. **[Hallazgo 2-a.]**

d. Corrija las fallas técnicas que propician que haya instituciones de la Administración en las que el SCP está inoperante. **[Hallazgo 2-b.]**

e. Instale los equipos necesarios en los centros alternos para asegurar la continuidad de servicio en caso de que una situación inusual o de emergencia impida el uso de las instalaciones del edificio principal de la Administración. **[Hallazgo 3-b.]**

f. Prepare un diagrama esquemático de la infraestructura de la red y se incluya copia de este en un área visible donde se encuentran los equipos computadorizados y de comunicaciones. **[Hallazgo 4-a.2) y c.1)]**

g. Realice las gestiones necesarias para que se organicen y se identifiquen los cables, de manera que se pueda determinar con facilidad a qué equipo pertenecen y corregir a tiempo los problemas de comunicación. **[Hallazgo 4-a.2), b.2) y c.1)]**

h. Corrija las deficiencias ambientales indicadas en el **Hallazgo 4-b.1) y c.2)**.

i. Efectúe las modificaciones en los parámetros de seguridad del sistema operativo de los servidores de la red para:

   1) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas. **[Hallazgo 5-a.1)a)]**

   2) Restringir a los usuarios el poder repetir las últimas cinco contraseñas utilizadas. **[Hallazgo 5-a.1)b)]**

3) Establecer que las contraseñas sean combinaciones alfanuméricas. **[Hallazgo 5-a.1)c)]**

4) Establecer un término de inactividad, de al menos 15 minutos, para que luego el sistema requiera una contraseña para continuar con el uso del mismo. **[Hallazgo 5-a.1)d)]**

5) Establecer un término, de al menos tres intentos de acceso sin éxito, para que el sistema deshabilite la cuenta de acceso. **[Hallazgo 5-a.1)e)]**

j. Evalúe las opciones correspondientes a las políticas de auditorías (*Audit Policy*), los privilegios a los usuarios (*User Rights Assignment*) y las opciones de seguridad (*Security Options*) y active las que considere necesarias de acuerdo con los riesgos y las amenazas de la entidad. **[Hallazgo 5-a.2)]**

k. Cumpla con lo establecido en el *Manual DCR-2009-02* en cuanto a la rotación cíclica de las cintas de los respaldos y al envío de las cintas al centro de respaldo alterno. **[Hallazgo 6-a.1) y 2)]**

l. Mantenga un registro de los respaldos realizados y de las cintas que se envían al centro alterno, que incluya lo indicado en el **Hallazgo 6-a.3)**.

m. Identifique y proteja las cintas de los respaldos, según lo indicado en el **Hallazgo 6-a.4)**.

n. Prepare y mantenga actualizado un registro de los programas adquiridos e instalados en las computadoras que incluya lo indicado en el **Hallazgo 7-b.**

2. Ejercer una supervisión efectiva sobre los superintendentes de las instituciones correccionales para que estos se aseguren de que se adiestren a los técnicos de récord de las instituciones en el uso del SCP para que cumplan con su responsabilidad de registrar la

información requerida por el sistema. Además, que se prepare y se les provea un manual de usuario que incluya los procedimientos de control de entrada de datos al SCP. **[Hallazgo 2-a.]**

3. Asegurarse de que se prepare un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones. Una vez este sea aprobado, tomar las medidas necesarias para que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Administración. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 3-a.]**

4. Coordinar con el personal del Departamento de Educación para que corrija la situación comentada en el **Hallazgo 4-a.1)**.

5. Ver que el Secretario Auxiliar de Administración y Gerencia se asegure de que el Encargado de la Oficina de Servicios Generales supervise a la Encargada de la Propiedad para que prepare y mantenga actualizado un inventario de la propiedad de la Administración, y se identifique y se marquen los equipos con un número de propiedad. **[Hallazgos 4-a.3), b.3) y c.3) y 7-a.]**

6. Asegurarse de que se establezcan cláusulas en los contratos de servicios para desarrollar sistemas computadorizados en las que se requiera la documentación que se indica en el **Hallazgo 8**.

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yamis M. Valdivieso

ANEJO

DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN
ADMINISTRACIÓN DE CORRECCIÓN
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Carlos M. Molina Rodríguez	Secretario de Corrección y Rehabilitación y Administrador de Corrección	2 jul. 10	29 abr. 11
Sr. Edgardo Centeno Soto	Secretario Auxiliar de Auditoría Interna	2 jul. 10	29 abr. 11
Sr. Francisco Suárez Martínez	Director Interino de Recursos Humanos[15]	24 ago. 10	29 abr. 11
Sra. Ana I. Escobar Pabón	Gerente de Administración	2 jul. 10	29 abr. 11
Sr. Ryan Vargas Alverio	Ayudante Especial en Presupuesto y Finanzas	2 jul. 10	29 abr. 11
Sr. Ángel Birriel Díaz	Especialista en Sistemas de Información[16]	2 jul. 10	29 abr. 11

[15] La Sra. Alice Carrero Carrero, Subdirectora de Recursos Humanos, estuvo a cargo de esa área del 2 de julio al 23 de agosto de 2011.

[16] El Sr. Ángel Birriel Díaz realizaba las funciones de Director de Sistemas de Información aunque no había una designación oficial.

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