#12514

SECRETARIO DEL SENADO

RECIBIDO MAY 02 2018 AM09:40

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR

Unidad 5214 : Corporación del Centro de las Bellas Artes de Puerto Rico
Oficina de Sistemas de Información

Informe número : TI-18-07 del 9 de abril de 2018

Período auditado : 13 de mayo de 2015 al 27 de mayo de 2016

Autorizado por : Yesmín Valdivieso
Yesmín M. Valdivieso, Contralora

Fecha : 16 de abril de 2018

El 9 de abril de 2018 aprobamos el *Informe de Auditoría TI-18-07*. Este contiene los resultados de la auditoría que realizamos en la Corporación del Centro de las Bellas Artes de Puerto Rico para determinar si las operaciones de la Oficina de Sistemas de Información se efectuaron de acuerdo con las normas generalmente aceptadas en este campo.

El *Informe* se puede conseguir en nuestra página en Internet: www.ocpr.gov.pr.

Notificación sobre Publicación de Informe en Internet

INFORME DE AUDITORÍA TI-18-07

9 de abril de 2018

Corporación del Centro de las Bellas Artes de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5214 - Auditoría 14022)

Período auditado: 13 de mayo de 2015 al 27 de mayo de 2016

CONTENIDO

Página

OBJETIVO DE AUDITORÍA **2**

CONTENIDO DEL INFORME **2**

ALCANCE Y METODOLOGÍA **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **4**

CONTROL INTERNO **5**

OPINIÓN Y HALLAZGOS **6**

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

2 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de las operaciones computadorizadas, y deficiencia en el Plan de Emergencias para los Sistemas de Información 8

3 - Deficiencias relacionadas con el mantenimiento de las cuentas de acceso a los recursos de la red y con los perfiles de seguridad establecidos para las mismas 11

4 - Deficiencias relacionadas con la producción, el almacenamiento y el control de los respaldos de información de la Corporación 14

5 - Falta de revisiones periódicas de los registros de eventos de seguridad 17

6 - Deficiencias relacionadas con los formularios de solicitud de acceso a la red, y con la justificación y la autorización de los accesos a las cuentas con privilegios de administración ... 18

7 - Programas instalados no autorizados y falta de inventario de programas instalados en las computadoras de la Corporación 20

8 - Falta de adiestramientos al analista y de un programa para divulgar al personal las normas y los procedimientos de seguridad de la información 23

9 - Incumplimiento de las recomendaciones incluidas en los informes de auditorías anteriores 25

RECOMENDACIONES **27**

APROBACIÓN **31**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **32**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **33**

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

9 de abril de 2018

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos de las operaciones de la Oficina de Sistemas de Información (OSI) de la Corporación del Centro de las Bellas Artes de Puerto Rico (Corporación). 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; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVO DE AUDITORÍA

Determinar si las operaciones de la OSI, en lo que concierne a los controles internos para la administración de la seguridad, el acceso lógico y físico, la continuidad del servicio, la segregación de deberes; y los equipos computadorizados, se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este es el primer informe, y contiene nueve hallazgos del resultado del examen que realizamos de las áreas indicadas en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 13 de mayo de 2015 al 27 de mayo de 2016. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestros hallazgos y opinión. En consecuencia, realizamos las pruebas que consideramos necesarias, a base

de muestras y de acuerdo con las circunstancias, según nuestro objetivo de auditoría. Realizamos pruebas 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.

En relación con el objetivo de la auditoría, consideramos que la evidencia obtenida proporciona una base razonable para nuestros hallazgos y opinión.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

Mediante la *Ley Núm. 43 del 12 de mayo de 1980* se creó la Corporación del Centro de las Bellas Artes de Puerto Rico como una corporación pública, cuya función principal consiste en administrar el complejo de salas de representación conocido como el Centro de las Bellas Artes (CBA). Dicha *Ley* fue enmendada por la *Ley Núm. 1 del 31 de julio de 1985* para disponer que de ahí en adelante la Corporación operará como un organismo autónomo adscrito al Instituto de Cultura Puertorriqueña. Mediante la *Ley 117-1993* se asignó al Centro de las Bellas Artes el nombre de Centro de Bellas Artes Luis A. Ferré Aguayo.

La Corporación comparte con el Instituto de Cultura Puertorriqueña la misma Junta de Directores (Junta). Esta se compone de nueve miembros quienes a su vez nombran al gerente general de la Corporación. El gerente general es el primer ejecutivo de la Corporación y la representa en todos sus actos y en los contratos que este otorga. La estructura organizacional de la Corporación se compone de las oficinas de Auditoría Interna, la cual responde a la Junta, del Gerente General, de Finanzas y Presupuesto, de Recursos Humanos, de Servicios Generales, de Sistemas de Información, de Programación y Servicios, de Estacionamiento y Transportación, y de la División de Alimentos y Bebidas.

A la fecha de nuestra auditoría, la OSI contaba con 1 analista programador de sistemas de información (analista), encargado de todas las operaciones de esta oficina, y 1 auxiliar de servicios generales, que brindaba apoyo a la misma. Además, tenía vacante el puesto de representante de información.

La Corporación contaba con una red de área local (LAN, por sus siglas en inglés) que brindaba servicios a las áreas operacionales y la Sala Sinfónica. Esta red consistía de cinco servidores físicos y uno virtual. La comunicación de los datos de la red se realizaba mediante una línea tipo T1 provista por la Oficina de Gerencia y Presupuesto (OGP).

Los recursos para financiar las actividades operacionales de la Corporación provenían de resoluciones conjuntas del presupuesto general, de asignaciones especiales del fondo general, y de ingresos propios. Para los años fiscales del 2013-14 al 2015-16, el presupuesto de la Corporación ascendió a $6,285,000, $5,746,000 y $4,939,000, respectivamente.

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

La Corporación cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.cba.pr.gov. 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* y otras situaciones determinadas durante la auditoría, fueron remitidas al Dr. Ricardo Cobián Figeroux, entonces gerente general de la Corporación, mediante cartas de nuestros auditores, del 6 de noviembre de 2015 y 7 de junio de 2016. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

El 30 de noviembre de 2015 y el 17 de junio de 2016, el doctor Cobián Figeroux contestó las cartas de nuestros auditores, y sus comentarios se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe* se remitió al Sr. Jetppeht Pérez de Corcho Morgado, gerente general de la Corporación, para comentarios, por carta del 2 de febrero de 2018. En el mismo se indicaron datos específicos, tales como los nombres de las cuentas de acceso a la red, y de programas. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al doctor Cobián Figeroux, ex gerente general.

El 13 de febrero el gerente general solicitó una prórroga para remitir sus comentarios, la cual concedimos hasta el 28 de febrero. Este contestó el borrador por carta del 27 de febrero. En los **hallazgos** se incluyeron algunos de sus comentarios.

El ex gerente general contestó el borrador de los **hallazgos** de este *Informe* por carta del 15 de febrero. En su contestación indicó, entre otras cosas lo siguiente:

> […] le comuniqué a las auditoras de mi renuncia al cargo de gerente general, efectivo el 30 de junio de 2016, apenas un mes después de que terminó la auditoría. La Sra. […] fue nombrada de inmediato gerente general interina, con el compromiso de darle seguimiento a los proyectos y asuntos administrativos que quedaron pendientes, incluyendo la auditoría. De igual manera, el analista […], quedó con la responsabilidad inmediata de seguir trabajando en el borrador del informe de auditoría de los sistemas de información del CBA. […] seguramente para esta fecha ya se deben haber corregido, sino todos, al menos algunos de los señalamientos conforme a los parámetros establecidos por su oficina. [*sic*]

CONTROL INTERNO

La gerencia de la Corporación es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para el objetivo de este *Informe*. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno de la Corporación.

En los **hallazgos del 1 al 8** de este *Informe* se comentan las deficiencias de controles internos significativas, dentro del contexto del objetivo de nuestra auditoría, identificadas a base del trabajo realizado. Además, en el **Hallazgo 9** se comenta otra deficiencia de control interno, sobre el incumplimiento de las recomendaciones incluidas en los informes de auditorías anteriores, la cual no es significativa para el objetivo de la auditoría, pero merece que se tomen acciones correctivas.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con el objetivo de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI de la Corporación, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 9** que se comentan a continuación.

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

Situación

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en una entidad, sus vulnerabilidades, y las amenazas a las que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas. Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implementados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, y proteger dichos activos, de manera que no se afecten adversamente las operaciones de la entidad. Mediante este proceso se asegura que

las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

Al 6 de octubre de 2015, en la Corporación no se había preparado un informe de análisis de riesgos de los sistemas de información computadorizados.

Criterios

La situación comentada se aparta de lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información,* de la *Carta Circular 77-05, Normas sobre la Adquisición e Implantación Tecnológica para los Organismos Gubernamentales,* aprobada el 8 de diciembre de 2004 por la directora de la OGP; y en la *Política TIG-015, Programa de Continuidad Gubernamental,* aprobada el 22 de septiembre de 2011 por el director de la OGP[1].

Efectos

La situación comentada impide a la Corporación estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, impide el desarrollo de un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable y los pasos a seguir para restablecer las operaciones de la Corporación en caso de que surja alguna eventualidad.

Causa

La situación comentada se atribuye a que el gerente general no había promulgado una directriz para la preparación y documentación de un análisis de riesgos que incluyera todos los activos de sistemas de información de la Corporación.

---

[1] La *Carta Circular 77-05* y la *Política TIG-015* fueron derogadas por la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales,* aprobada el 7 de noviembre de 2016 por el director de la OGP. Esta contiene disposiciones similares a las de la *Carta Circular* y *Política* derogadas.

Comentarios de la Gerencia

El gerente general nos indicó las medidas que están en proceso para corregir la situación comentada.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de las operaciones computadorizadas, y deficiencia en el Plan de Emergencias para los Sistemas de Información

Situaciones

a. Al 5 de octubre de 2015, la Corporación carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la OSI. Esto es necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la Corporación, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. Al 29 de septiembre de 2015, la Corporación no contaba con un centro alterno para recuperar sus operaciones críticas computadorizadas en caso de emergencia.

c. La OSI contaba con el *Plan de Emergencias para los Sistemas de Información* (*Plan*), el cual incluía las acciones a tomar durante los diferentes tipos de emergencias, tales como: huracanes, fuegos, terremotos, fallas en los equipos, y protestas de empleados, entre otras. Además, incluía las instrucciones para realizar los respaldos de los servidores de la Corporación, y el plan de restauración de acuerdo a los tipos de emergencia. Este *Plan* fue preparado por el analista y aprobado por la gerente general el 25 de enero de 2007.

   El examen realizado el 11 de agosto de 2015 sobre el contenido del *Plan* reveló que este no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

   - Un inventario de equipos y de archivos críticos del área de sistemas de información

- El detalle del contenido de los respaldos, así como los nombres de las librerías y de los archivos
- Un itinerario de restauración que incluya el orden de los programas a restaurar
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05* y en la *Política TIG-015*.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del plan de continuidad del negocio, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse 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 agencia.

Estas prácticas también sugieren que, como parte del plan de continuidad de negocios, se prepare un plan de contingencias. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afecten su funcionamiento. El mismo deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado c.]**

Efectos

Las situaciones comentadas en los **apartados a. y c.** pueden propiciar la improvisación, y que en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos y de interrupciones prolongadas de los servicios ofrecidos a los usuarios de la Corporación.

La situación comentada en el **apartado b.** podría afectar las operaciones de la Corporación, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la OSI.

Causas

La situación comentada en el **apartado a.** se atribuye a la falta de un análisis de riesgos de los sistemas de información computadorizados de la Corporación que sirviera de base para la preparación y la revisión de un plan de continuidad de negocios. **[Véase el Hallazgo 1]**

Las situaciones comentadas en los **apartados b. y c.** se atribuyen a que el analista no había realizado las gestiones necesarias para:

- Identificar un lugar disponible y adecuado como centro alterno, y formalizar los acuerdos necesarios para la utilización del mismo en casos de emergencia. **[Apartados b.]**

- Incluir en el *Plan* los requisitos mencionados. **[Apartado c.]**

Comentarios de la Gerencia

El gerente general indicó lo siguiente:

> Como centro alterno la data que manejan los usuarios de la corporación, al igual que el correo electrónico se encuentra hospedado en la nube con office365. En caso de emergencia en la que se necesite trabajar con dicha data por cualquier situación crítica la misma podrá ser utilizada en la nube para continuar con las labores. [*sic*] **[Apartado b.]**

Consideramos las alegaciones del gerente general con respecto al **apartado b.**, pero determinamos que el mismo prevalece. Esto, debido a que durante el examen realizado encontramos que los programas esenciales de la Corporación que incluyen los sistemas de contabilidad, de venta de boletos y de control de acceso al estacionamiento; no se mantenían almacenados en la nube.

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

Hallazgo 3 - Deficiencias relacionadas con el mantenimiento de las cuentas de acceso a los recursos de la red y con los perfiles de seguridad establecidos para las mismas

Situaciones

a. Del 1 de julio de 2011 al 30 de junio de 2015 en la Corporación cesaron en sus funciones 33 empleados. El examen realizado el 11 de agosto de 2015 sobre el estatus de las cuentas de acceso otorgadas a estos exempleados reveló lo siguiente:

    1) No se habían desactivado las cuentas de acceso de 3 exempleados que cesaron sus funciones el 30 de junio de 2015, el 31 de marzo de 2015 y el 30 de junio de 2013. A la fecha del examen, habían transcurrido 42, 133 y 772 días, respectivamente, desde la separación de estos exempleados. La cuenta de uno de estos exempleados tenía privilegios de administración[2].

    2) Las cuentas de acceso de 5 exempleados[3] fueron utilizadas luego de su fecha de separación. El acceso a la red mediante el uso de estas cuentas ocurrió entre 8 y 92 días posteriores a la fecha de separación de estos.

[2] Privilegios que permiten acceso sin restricciones, a través de los sistemas operativos, para efectuar cambios que afectan a otros usuarios, tales como: modificar la configuración de la seguridad, instalar programas y equipos, acceder a todos los archivos en un equipo y realizar cambios en las cuentas de acceso.

[3] La cuenta de uno de estos exempleados tenía privilegios de administración.

Las transacciones realizadas mediante estas cuentas no se pudieron examinar debido a que en la Corporación no se realizaba un respaldo al registro de eventos de seguridad *(security event log)*. **[Véase el Hallazgo 4-a.2)]**

b. Al 11 de agosto de 2015, en el *Primary Domain Controller* (PDC)[4] había 77 cuentas de usuario para acceder a la red. El examen realizado sobre los perfiles de seguridad establecidos individualmente para estas cuentas reveló las siguientes deficiencias:

1) Las contraseñas de 10 cuentas (13%) no se habían cambiado luego de haber transcurrido más de 365 días desde la fecha en que fueron establecidas. El tiempo transcurrido fluctuaba entre los 389 y 1,037 días. Entre estas cuentas había 3 que tenían privilegios de administración.

2) Trece cuentas (17%) estaban configuradas para que no expiraran *(Password Expires: No)*, lo que permitía a los usuarios de estas mantener la misma contraseña por tiempo indefinido *(Password Expire Time: Never)*. Entre estas cuentas había tres que tenían privilegios de administración.

3) Siete cuentas (9%) nunca habían sido utilizadas por sus usuarios *(Never logon - Last Logon Time).*

4) Cinco cuentas (6%) permanecían activas a pesar de que habían transcurrido entre 137 y 883 días luego de su última conexión *(Last Logon Time)*. Una de estas cuentas tenía privilegios de administración.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las entidades gubernamentales deberán implementar controles que minimicen los riesgos de que los sistemas de información

[4] Servidor mediante el cual se controla el acceso a los recursos de la red.

dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Dicha norma se establece, en parte, mediante lo siguiente:

- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente. **[Apartado a.]**
- La desactivación inmediata de todas las cuentas de acceso que no estén en uso. **[Apartados a. y b.4)]**
- La revisión periódica de las cuentas activas en los sistemas de información de la Corporación. **[Apartados a. y b.]**
- El mantenimiento de registros confiables y actualizados de las cuentas solicitadas y autorizadas. **[Apartado a.]**
- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos. **[Apartado b.]**
- El establecimiento de fechas de expiración a las contraseñas de las cuentas de acceso para obligar y permitir al usuario cambiar las mismas. **[Apartado b.1) y 2)]**

Efectos

Las situaciones comentadas pueden propiciar que personas no autorizadas accedan información confidencial y hagan uso indebido de esta, y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados. Esto, sin que se puedan detectar a tiempo para fijar responsabilidades.

Causas

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

de acceso se mantuvieran actualizados. Además, la Corporación no contaba con normas o procedimientos relacionados con la transferencia o separación del personal.

Las situaciones comentadas en el **apartado b.** se debían, en parte, a que el analista no había establecido controles adecuados para el mantenimiento de las cuentas de acceso a la red, y de las que tenían privilegios de administración.

Véanse las recomendaciones 1, 4 de la c. a la e., y 5.a. y b.

Hallazgo 4 - Deficiencias relacionadas con la producción, el almacenamiento y el control de los respaldos de información de la Corporación

Situaciones

a. Al 29 de septiembre de 2015, el analista era el responsable del proceso de respaldo de la información mantenida en los servidores de la Corporación. Los respaldos preparados incluían los documentos de los usuarios, la configuración del *ISA Server*[5], los correos electrónicos, y la base de datos de la aplicación financiera, utilizada por la Oficina de Finanzas y Presupuesto. Estos respaldos se preparaban diariamente (incrementales)[6] y mensualmente (completos), mediante el programa de libre distribución instalado en el PDC de la Corporación.

   Los respaldos se grababan en un equipo de cuatro discos, mediante un proceso de imagen. En este equipo se mantenían tres de estos discos y el otro se debía llevar mensualmente a una compañía externa, a la que se pagaba un alquiler de $300 anuales por una caja de seguridad.

[5] *Internet Security and Acceleration Server*. En este se analiza el encabezado de los paquetes de protocolo de Internet (IP) en busca de tráfico sospechoso.

[6] Se copian únicamente los archivos y directorios creados o modificados desde el último respaldo realizado.

El examen sobre la preparación, el almacenamiento y el control de los respaldos de información reveló las siguientes deficiencias:

1) No se preparaban respaldos de los archivos relacionados con el manejo de las asistencias del personal y el registro de transacciones del estacionamiento.

2) No se respaldaban los registros de eventos de seguridad de los sistemas operativos *(security event logs)*[7] y de los accesos a Internet, que permitieran conservar esta información histórica.

3) Durante el período del 1 de julio de 2010 al 11 de mayo de 2015, no se enviaron los respaldos de información a la compañía externa. Esto a pesar de que durante este período, la Corporación le pagó a dicha compañía por el alquiler de la caja de seguridad para almacenar los respaldos.

4) No se mantenía un registro de los respaldos preparados en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor donde se mantenían, 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.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las agencias deben establecer controles adecuados en sus sistemas de información para garantizar la confidencialidad, integridad y disponibilidad de la información que manejan. Además, se establece que deberán existir procedimientos para tener y mantener una copia de respaldo recurrente de la información y de los programas de aplicación y de sistema, esenciales e importantes para las operaciones de la agencia. En consonancia con dicha política pública es necesario, entre otras cosas, que

[7] Este registro puede mantener acontecimientos sobre seguridad, tales como: intentos válidos e inválidos de conexión, y acontecimientos relacionados con el uso del recurso, como crear, abrir, o suprimir archivos. Un administrador puede especificar qué acontecimientos se mantienen en el registro de seguridad.

toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. Además, es necesario mantener un inventario detallado de las cintas de respaldos para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para los respaldos.

Efectos

La situación comentada en el **apartado a.1)** podría ocasionar la pérdida permanente de información importante, sin la posibilidad de poder recuperarla, lo que afectaría adversamente las operaciones de la Corporación.

La situación comentada en el **apartado a.2)** limitaba el acceso de la Corporación a la información histórica y las transacciones relacionadas con eventos de seguridad de los sistemas operativos y accesos a Internet.

La situación comentada en el **apartado a.3)** puede ocasionar que, en casos de emergencia, la Corporación no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones. Además, como resultado de esta situación la Corporación no obtuvo beneficio de los $1,500 pagados a la compañía externa por el arrendamiento de la caja de seguridad.

La situación comentada en el **apartado a.4)** dificulta la localización e identificación del contenido de las cintas de respaldos, lo que podría afectar el proceso de restauración de los sistemas en caso de contingencias o emergencias. Además, limitó el alcance de nuestro examen para determinar si los respaldos se habían preparado con la regularidad requerida.

Causas

Las situaciones comentadas se debían a que el analista no le dio la atención correcta al proceso de preparar, almacenar y controlar los respaldos. Además, la Corporación no contaba con procedimientos

escritos, que incluyeran las directrices específicas y detalladas para producir y almacenar los respaldos con la información crítica, y para mantener un registro adecuado de los mismos.

Véanse las recomendaciones 1 y 4 de la f. a la i.

Hallazgo 5 - Falta de revisiones periódicas de los registros de eventos de seguridad

Situación

a. Al 29 de septiembre de 2015, el analista no examinaba periódicamente los registros de seguridad provistos por el sistema operativo. Esto es necesario para conocer las posibles violaciones de seguridad que pudieran ocurrir en el servidor y en la red, y tomar prontamente las medidas preventivas y correctivas necesarias. El analista sólo examinaba dichos registros en el caso de que ocurriera alguna eventualidad con los sistemas de información.

Criterio

La situación comentada se aparta de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las entidades gubernamentales deberán implementar 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. Esta norma se establece, en parte, mediante el examen continuo de los registros que detallan los eventos inusuales del sistema.

Efecto

La falta de verificaciones periódicas de los registros que provee el sistema operativo priva a la Corporación de las herramientas necesarias para detectar irregularidades y alteraciones, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados, sin que se puedan detectar a tiempo para fijar responsabilidades.

Causas

Lo comentado se debió, en parte, a que el analista realizaba todas las funciones relacionadas con los sistemas de información de la Corporación, por lo que se le hacía difícil la revisión periódica de los registros de

seguridad, y solo los revisaba cuando ocurrían situaciones irregulares. Además, se atribuye a que el analista no recibía adiestramientos sobre los temas relacionados con las funciones que se le habían asignado. **[Véase el Hallazgo 8-a.]**

Véanse las recomendaciones 1 y 4.j.

Hallazgo 6 - Deficiencias relacionadas con los formularios de solicitud de acceso a la red, y con la justificación y la autorización de los accesos a las cuentas con privilegios de administración

Situaciones

a. Desde noviembre de 2011, la Corporación estableció en las *Normas y Procedimientos para el Uso del Equipo Computadorizado*, la utilización del formulario *Solicitud de Acceso a Cuentas Sistema Computadorizado*. Esto para la creación de las cuentas de acceso de los usuarios a los sistemas de información. Además, en este formulario se documentaba si el personal necesitaba acceso a Internet, para lo cual también debían completar el formulario *Permiso de Utilización de Internet*. El usuario también debía firmar la *Advertencia para el Uso del Sistema de Información Computadorizado*. Esta incluía las medidas de seguridad, que el usuario reconocía haber leído y entendido, al aceptar utilizar una computadora en la Corporación. Los formularios debían ser completados por el solicitante y su supervisor, y aprobados por el gerente general o su representante autorizado. Luego se entregaban al analista, quien era el responsable de crear y dar mantenimiento a las cuentas de acceso a la red, y de otorgar los permisos para acceder a Internet.

   El examen realizado al 7 de octubre de 2015 sobre el proceso para solicitar y autorizar la creación de las cuentas de acceso a la red e Internet de 15 usuarios, reveló que para 14 de estas no se habían preparado la *Solicitud de Acceso a Cuentas Sistema Computadorizado* ni el *Permiso de Utilización de Internet*.

b. Al 21 de septiembre de 2015, el analista no suministró para examen los documentos justificantes autorizados para otorgar los privilegios de administrador a las cinco cuentas de acceso que los tenían

asignados. Los privilegios otorgados a estas cuentas les permitía a los usuarios, entre otras cosas, configurar la seguridad del sistema de información, administrar las cuentas de acceso e iniciar o cancelar servicios.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en el inciso I.1.e) y 5.a) de las *Normas y Procedimientos para el Uso del Equipo Computadorizado,* aprobadas el 4 de noviembre de 2011 por la Junta. En este se dispone, entre otras cosas, que para tener acceso al sistema de computadoras de la Corporación y sus servicios asociados, el usuario deberá tener debidamente formalizado el formulario *Solicitud de Acceso a Cuentas Sistema Computadorizado,* y el acceso a Internet estará limitado a ciertos funcionarios, según lo autorice el gerente general de la Corporación mediante el formulario *Permiso de Utilización de Internet*. Además, requiere que cada uno de los usuarios debe firmar la *Advertencia para el Uso del Sistema de Información Computadorizado*.

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

- Las entidades gubernamentales deberán implementar 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. **[Apartados a. y b.]**

- La información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de manera que solamente el personal autorizado pueda ver los datos necesarios, o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deberán incluir mecanismos de autenticación y autorización. **[Apartado b.]**

Efectos

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios. También pueden propiciar que personas no autorizadas logren

acceso a información confidencial y hagan uso indebido de esta; y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que puedan detectarse a tiempo para fijar responsabilidades.

Causas

La situación comentada en el **apartado a.** se debía a que el analista no requirió el uso de los formularios para la creación de las cuentas comentadas.

Lo comentado en el **apartado b.** se debía a que la Corporación no contaba con un formulario para solicitar y autorizar la creación de cuentas de acceso con privilegios de administración.

Véanse las recomendaciones 1, y 4.k. y l.

Hallazgo 7 - Programas instalados no autorizados y falta de inventario de programas instalados en las computadoras de la Corporación

Situaciones

a. El 23 de septiembre de 2015 el analista nos entregó el informe *CBA: Applications by Computer*. Este informe incluía el detalle de los programas instalados en 54 computadoras y 7 servidores, que estaban conectados a la red al momento de producir el mismo.

   Identificamos las 5 computadoras con mayor cantidad de programas instalados. El examen de los programas instalados en estas computadoras reveló que existían 68 programas que no fueron autorizados por la Corporación ni guardaban relación con los trabajos que se realizaban en esta.

b. Al 30 de septiembre de 2015, la Corporación no mantenía un inventario completo y actualizado de los programas adquiridos e instalados en las computadoras, que al menos incluyera el número de la licencia, el nombre del proveedor, la fecha de adquisición, el número de propiedad asignado, la identificación del equipo donde estaba instalado y su localización, y el nombre del usuario o custodio del mismo.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en los incisos I.D. y F. de las *Normas y Procedimientos para el Uso del Equipo Computadorizado*. En estos se prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización válida a nombre de la Corporación, y la instalación de programas en las computadoras, sin la autorización por escrito del gerente general o su representante autorizado.

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la *Carta Circular 77-05*. En esta se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que debe constar en el inventario de las respectivas entidades gubernamentales y sólo pueden utilizarse para fines estrictamente oficiales y legales. Además, las mejores prácticas de la tecnología de información sugieren que se mantenga un registro de todos los programas en el cual se indique lo siguiente: el número de la licencia, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el equipo donde está instalado (número de propiedad o de serie), la ubicación física de la licencia y de sus manuales, el nombre del usuario, el número de propiedad asignado, y el costo.

Efectos

Lo comentado en el **apartado a.** reduce el espacio y la capacidad en los sistemas de información de la Corporación, lo que podría afectar el rendimiento de los mismos. Por otro lado, expone a los equipos y a la información sensitiva almacenada en los sistemas, a riesgos innecesarios como son la propagación de virus, *spyware*[8], *phishing*[9],

[8] 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.

[9] 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.

spoofing[10], *spamming*[11] y ataques de negación de servicios[12], entre otros, que pudieran afectar la continuidad de las operaciones de la Corporación, sin que se puedan fijar responsabilidades.

La situación comentada en el **apartado b.** le impide a la Corporación ejercer un control eficaz de los programas y sus licencias. Esto, a su vez, propició la instalación y el uso de programas no autorizados, sin que se pudiera detectar a tiempo para fijar responsabilidades.

Causas

La situación comentada en el **apartado a.** se atribuye en parte a que el analista no había recibido adiestramientos, entre otras cosas, sobre los controles que se debían establecer para la instalación de programas **[Véase el Hallazgo 8-a.]**.

Además, las situaciones comentadas se atribuyen a que el gerente general no se aseguró de que el analista:

- Estableciera controles efectivos que limitaran el acceso a la opción *Add/Remove Programs* del sistema operativo en las computadoras, para impedir la instalación de programas no autorizados. **[Apartado a.]**
- Mantuviera un registro de inventario completo y actualizado de los programas autorizados e instalados en las computadoras. **[Apartado b.]**

---

[10] 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.

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

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

Comentarios de la Gerencia

El gerente general indicó lo siguiente:

> Actualmente nos encontramos haciendo un análisis de los equipos computadorizados que tenemos en la Corporación para identificar que cada computadora tenga los programas que solo se utilizan para labores rutinarias […]. **[Apartado a.]**

Véanse las recomendaciones 1, y 4.m. y n.

Hallazgo 8 - Falta de adiestramientos al analista y de un programa para divulgar al personal las normas y los procedimientos de seguridad de la información

Situaciones

a. El Analista, quien administraba la red de la Corporación, no había recibido adiestramientos para realizar las tareas que se le habían asignados relacionadas con:

- Los sistemas operativos
- Los protocolos de la red
- El diseño, la instalación, la configuración y el mantenimiento de la red
- El monitoreo de la red, las herramientas para la autoevaluación de la misma y la detección de intrusos
- El análisis de problemas
- Las actualizaciones o mejoras en los sistemas
- Las nuevas amenazas y posibles soluciones
- La seguridad y confidencialidad de la información.

Estos adiestramientos son necesarios para asegurar que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con la seguridad de los sistemas de información.

b. Al 20 de mayo de 2016, la Corporación no contaba con un programa para divulgar al personal las normas y los procedimientos de seguridad de la información (*security awareness*). Mediante este se orienta a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la entidad y se da a conocer la reglamentación y la política pública relacionadas con la seguridad de la misma.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*, en la que se establece, entre otras cosas, que el personal de sistemas de información y telecomunicación deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.

Las mejores prácticas en el campo de la tecnología de información requieren que cada entidad gubernamental establezca e implemente un programa para la divulgación de las normas y los procedimientos de seguridad de información a todos sus funcionarios y empleados. Un programa bien diseñado para la divulgación de las normas y los procedimientos de seguridad debe estar, primeramente, encaminado a crear conciencia de los riesgos a los cuales están expuestos los sistemas de información, y luego a desarrollar actitudes prácticas en los funcionarios y los empleados de una organización con el fin de promover la protección de los activos físicos y los de la información. La concienciación de los riesgos y las salvaguardas disponibles son las primeras líneas de defensa que se utilizan en la seguridad de los sistemas de información y de las redes de comunicación gubernamentales. **[Apartado b.]**

Efectos

La situación comentada en el **apartado a.** propició la falta de revisiones periódicas de los registros de eventos de seguridad comentadas en el **Hallazgo 5**, y de controles sobre los programas instalados en las computadoras incluidas en el **Hallazgo 7-a.** Además, ocasionaba el desconocimiento y la falta de entendimiento, por parte del analista, de las responsabilidades relacionadas con la seguridad y protección de los sistemas

computadorizados. Esto, podría reducir la efectividad de dichos sistemas y exponer la información a riesgos innecesarios que afecten la continuidad de las operaciones de la Corporación.

La situación comentada en el **apartado b.** podría ocasionar el incumplimiento de las normas de seguridad con los consiguientes efectos adversos en cuanto a la protección de la información. Esto, a su vez, podría afectar la integridad, disponibilidad y confiabilidad de la información procesada por los usuarios.

Causas

Las situaciones comentadas se atribuyen a que el gerente general:

- No se aseguró de que el analista recibiera los adiestramientos necesarios para realizar las funciones que le fueron asignadas. **[Apartado a.]**
- No le requirió a la gerente auxiliar de Recursos Humanos que implementara un programa para orientar a todos los empleados de la Corporación con relación a las normas y los procedimientos de seguridad de la información. **[Apartado b.]**

Comentarios de la Gerencia

El gerente general indicó lo siguiente:

> Se están realizando las gestiones con la Oficina de Gerencia y Presupuesto para saber la disponibilidad de cursos técnicos. Esta es nuestra primera alternativa, debido a que estos cursos no habría que pagarlos, ya que la OGP se encarga de esta parte. […]
>
> En adición se comenzó a realizar una búsqueda de posibles compañías privadas que puedan ofrecer estos talleres o cursos […]. **[Apartado a.]**

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

Hallazgo 9 - Incumplimiento de las recomendaciones incluidas en los informes de auditorías anteriores

Situaciones

a. En el examen realizado sobre los controles establecidos para la administración del control de acceso lógico y físico, y la continuidad del servicio identificamos situaciones similares a las que fueron

señaladas en informes de auditoría anteriores. Esto, a pesar de que en los planes de acción correctiva presentados por la Corporación a nuestra Oficina, se indicaba que las recomendaciones incluidas en dichos informes, habían sido cumplimentadas, según se indica:

1) En el *Informe de Auditoría TI-02-06* del 12 de diciembre de 2001 fue objeto de recomendación una situación relacionada con la falta de un plan de continuidad de negocios, que incluyera los planes específicos, completos y actualizados de la OSI. En el plan de acción correctiva de dicho *Informe*, realizado al 7 de mayo de 2002, se indicó que se había cumplimentado la recomendación dirigida a corregir esta situación. Sin embargo, durante nuestra auditoría determinamos que la misma no habían sido corregida. **[Véase el Hallazgo 2-a.]**

2) En el *Informe de Auditoría TI-03-11* del 19 de mayo de 2003 fueron objeto de recomendaciones situaciones relacionadas con deficiencias en el proceso de solicitud y autorización para la creación de las cuentas de acceso. En el plan de acción correctiva de dicho *Informe*, realizado al 7 de mayo de 2005, se indicó que la recomendación para corregir estas situaciones se había cumplimentado. Sin embargo, durante nuestra auditoría determinamos que dichas situaciones aún persistían en la Corporación. **[Véase el Hallazgo 6-a.]**

Criterio

Las normas para una sana administración pública requieren que los jefes de las entidades gubernamentales cumplan con las recomendaciones incluidas en los informes de auditores internos o externos. Esto, con el propósito de tomar a tiempo las medidas correctivas necesarias sobre las deficiencias comentadas y evitar que las mismas se repitan.

Efecto

Las situaciones comentadas podrían poner en riesgo los sistemas de información computadorizados y las operaciones principales de la Corporación.

Causa

Lo comentado se debió, en parte, a que el analista realizaba todas las funciones relacionadas con los sistemas de información de la Corporación, lo que dificultó la atención de las recomendaciones.

Comentarios de la Gerencia

El gerente general indicó lo siguiente:

> Es nuestro interés y compromiso de que se cumpla con las normas y reglamentos para una sana administración pública. Estaremos trabajando un plan para la revisión y cumplimiento de las recomendaciones indicadas por la Oficina del Contralor.

Véanse las recomendaciones 1 y 7.

RECOMENDACIONES

A la Junta de Directores del Instituto de Cultura Puertorriqueña

1. Ver que el gerente general de la Corporación cumpla con las **recomendaciones de la 2 a la 7** de este *Informe*. **[Hallazgos del 1 al 9]**

Al Gerente General de la Corporación del Centro de las Bellas Artes de Puerto Rico

2. Asegurarse de que se realice y documente un análisis de riesgos de los sistemas de información computadorizados de la Corporación, según se establece en las políticas *ATI-003, Seguridad de los Sistemas de Información*, y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*. El informe producto de este análisis de riesgos, debe ser remitido para revisión y aprobación de la Junta. Una vez aprobado, ver que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de la Corporación, para asegurarse de que se mantenga actualizado. **[Hallazgo 1]**

3. Asegurarse de que se realicen las gestiones necesarias para 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. Este plan debe ser remitido para revisión y aprobación de la Junta. Una vez este sea aprobado, tomar las medidas necesarias

para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Corporación. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 2-a.]**

4. Ejercer una supervisión efectiva sobre el analista para asegurarse de que:

   a. Identifique un lugar y establezca un centro alterno que cuente con el equipo necesario para restaurar las operaciones críticas de la OSI en caso de desastres o emergencias. **[Hallazgo 2-b.]**

   b. Revise el *Plan de Emergencias para los Sistemas de Información,* lo actualice para incluir los requisitos mencionados en el **Hallazgo 2-c.**, y lo remita para su consideración y la aprobación de la Junta. Una vez aprobado, velar por que se divulgue a los funcionarios y a los empleados concernientes, y que se realicen evaluaciones periódicas del mismo para asegurar su funcionamiento.

   c. Desactive las cuentas de acceso de los exempleados, y cualquier otro personal que concluya sus labores en la Corporación, y ver que, en lo sucesivo, se desactiven en el momento en que el usuario cese sus funciones. **[Hallazgo 3-a.]**

   d. Efectúe las modificaciones en los parámetros de seguridad del sistema operativo del servidor principal para que se habilite la función de expiración a todas las contraseñas de las cuentas de acceso de los usuarios. **[Hallazgo 3-b.1) y 2)]**

   e. Elimine o desactive, si aún no lo ha hecho, las cuentas de acceso que nunca se han conectado a la red de comunicación y las que no se han utilizado durante períodos mayores de 90 días. **[Hallazgo 3-b.3) y 4)]**

f. Prepare y remita para su consideración y la aprobación de la Junta los procedimientos escritos necesarios que permitan establecer directrices específicas y detalladas para producir y almacenar las copias de respaldos, y para mantener un registro adecuado de las mismas. **[Hallazgo 4]**

g. Prepare los respaldos de la información crítica y de los registros de eventos de seguridad de la Corporación que se comentan en el **Hallazgo 4-a.1) y 2)**.

h. Mantenga una copia de los respaldos en la caja de seguridad de la compañía externa o en un lugar externo, para salvaguardar la información de los sistemas computadorizados de la Corporación. **[Hallazgo 4-a.3)]**

i. Prepare un registro de los respaldos realizados que le permita controlar y documentar adecuadamente la preparación de estos. Además, se asegure de que el registro contenga la información que se indica en el **Hallazgo 4-a.4)**.

j. Revise y documente las revisiones realizadas a los registros de seguridad *(security event log)* y de ser necesario, tome de inmediato las medidas preventivas y correctivas. **[Hallazgo 5]**

k. Se asegure de que los formularios requeridos por las *Normas y Procedimientos para el Uso del Equipo Computadorizado* se preparen y autoricen previo a la creación y la modificación de las cuentas. Además, de que dichos formularios sean cumplimentados en todas sus partes. **[Hallazgo 6-a.]**

l. Prepare un formulario, o establezca alguna otra forma de documentación, para justificar y autorizar las cuentas de acceso con privilegios de administración, previo a su creación y modificación. **[Hallazgo 6-b.]**

m. Efectúe las modificaciones en los parámetros de seguridad del sistema operativo del servidor principal para que establezca los controles necesarios para restringir el acceso de los usuarios de

las computadoras mediante la opción de *Add/Remove Programs*. Esto, para que los usuarios no puedan instalar o remover programas. **[Hallazgo 7-a.]**

n. Prepare y mantenga un registro completo y actualizado de los programas autorizados e instalados en las computadoras de la Corporación. **[Hallazgo 7-b.]**

5. Ejercer una supervisión efectiva sobre la gerente auxiliar de Recursos Humanos para asegurarse de que:

a. Redacte las normas y los procedimientos necesarios para establecer controles para el manejo de la terminación y transferencia de los empleados de la Corporación. En los mismos se debe considerar, entre otras cosas, la notificación inmediata a la OSI del cese de un usuario en sus funciones, o de la modificación de las mismas. Las normas y los procedimientos deben ser remitidos para su consideración y la aprobación de la Junta. **[Hallazgo 3-a.]**

b. Notifique a la OSI el cese de los empleados en sus funciones, para la cancelación inmediata de las cuentas de acceso de estos. **[Hallazgo 3-a.]**

c. Establezca un programa de capacitación para orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la Corporación y dar a conocer la reglamentación y las políticas relacionadas con la seguridad de la información. **[Hallazgo 8-b.]**

6. Asegurarse de que el analista reciba los adiestramientos necesarios para realizar las funciones que le fueron asignadas. **[Hallazgo 8-a.]**

7. Asegurarse de que se tomen las medidas necesarias para que no se repitan las situaciones comentadas, y se atiendan las recomendaciones de los informes de nuestra Oficina. **[Hallazgo 9]**

APROBACIÓN

A los funcionarios y a los empleados de la Corporación, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

ANEJO 1

CORPORACIÓN DEL CENTRO DE LAS BELLAS ARTES 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
Dr. José L. Ramos Escobar	Presidente	13 may. 15	27 may. 16
Dra. Mareia Quintero Rivera	Vicepresidenta	13 may. 15	27 may. 16
Dr. José L. Vargas Vargas	Secretario	18 sep. 15	27 may. 16
Sra. Cynthia Montalvo Martínez	Secretaria[13]	13 may. 15	21 ago. 15
Dr. Lucas Mattei Rodríguez	Subsecretario	13 may. 15	27 may. 16
Dr. José L. Vargas Vargas	Miembro	13 may. 15	17 sep. 15
Lcdo. Michel Godreau Álvarez	"	13 may. 15	27 may. 16

[13] Este puesto estuvo vacante del 21 de agosto de 2015 al 17 de septiembre de 2016.

ANEJO 2

CORPORACIÓN DEL CENTRO DE LAS BELLAS ARTES DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Ricardo Cobián Figeroux	Gerente General	13 may. 15	27 may. 16
Sra. Idalia Martínez Martínez	Gerente Auxiliar de Recursos Humanos	13 may. 15	27 may. 16
Sr. Rafael Santos Picó	Gerente Auxiliar de Finanzas	13 may. 15	27 may. 16
Sra. Carmen Cúas Velázquez	Gerente Auxiliar de Servicios Generales, Interina	1 ene. 16	27 may. 16
Sra. Constancia Ramos Román	"	13 may. 15	31 dic. 15
Sr. José A. Negrón Hernández	Analista Programador de Sistemas de Información	13 may. 15	27 may. 16
Sra. Sarahí Matos Carrillo	Auditora Interna	13 may. 15	27 may. 16

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, extensiones 2801 o 2805, 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 y el tipo de opinión del informe.

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 787-754-3030, extensión 3400.

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:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr