Estado Libre Asociado de Puerto Rico
Oficina del Contralor

#14365

RECIBIDO APR1 '19 AM11:13
SECRETARIA DEL SENADO

14984

Yesmín M. Valdivieso
Contralora

PRESIDENCIA DEL SENADO

RECIBIDO MAR29'19 PM 3:24

Vmcv

29 de marzo de 2019

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-19-06* de los sistemas de información computadorizados de la Corporación de las Artes Musicales, aprobado por esta Oficina el 26 de marzo de 2019. Publicaremos dicho *Informe* en nuestra página en Internet: 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: www.ocpr.gov.pr
www.facebook.com/ocpronline *www.twitter.com/ocpronline*

INFORME DE AUDITORÍA TI-19-06

26 de marzo de 2019

Corporación de las Artes Musicales

Sistemas de Información Computadorizados

(Unidad 5207 - Auditoría 14195)

Período auditado: 1 de mayo de 2017 al 26 de enero de 2018

CONTENIDO

Página

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

26 de marzo de 2019

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 los sistemas de información computadorizados de la Corporación de las Artes Musicales (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*.

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones de la Corporación, en lo que concierne a los sistemas de información computadorizados, se efectuaron de acuerdo con las normas y la reglamentación aplicables.

Objetivo específico

Determinar si los controles establecidos para los sistemas de información computadorizados de la Corporación; relacionados con el análisis de riesgos; el manejo de incidentes; las solicitudes, las autorizaciones y el monitoreo de los accesos a la red, Internet y el correo electrónico; la continuidad del servicio; el registro de programas adquiridos y autorizados; y el mantenimiento preventivo de los equipos de la red de comunicación; se efectuaron de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este *Informe* contiene cuatro hallazgos del resultado del examen que realizamos de los objetivos indicados en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de mayo de 2017 al 26 de enero de 2018. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas tales como: entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la entidad auditada; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

Al realizar esta auditoría, utilizamos 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 Oficina de Gerencia y Presupuesto. Para las áreas relacionadas con el centro alterno para restaurar las operaciones y el almacenamiento de los respaldos **[Hallazgos 2-b. y 3]**, que no estaban consideradas en dichas políticas, utilizamos como mejor práctica las guías establecidas en el *Federal Information System Controls Audit Manual* (*FISCAM*)[1], emitido por el GAO. Esto, porque aunque a la Corporación no se le requiere cumplir con dichas guías, entendemos que estas representan

[1] El *FISCAM* está de acuerdo con las guías emitidas por el *National Institute of Standards and Technology*, entre estas, la publicación especial 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* y 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*.

las mejores prácticas en el campo de la tecnología de información, al examinar los sistemas computadorizados de las entidades gubernamentales.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgos.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Corporación fue creada mediante la *Ley Núm. 4 del 31 de julio de 1985*, *Ley de la Corporación de las Artes Musicales*, según enmendada, con la misión de promover y fomentar el desarrollo y enriquecimiento de la música y de las artes escénico-musicales en Puerto Rico. La Corporación cuenta con dos corporaciones subsidiarias[2], la Corporación de las Artes Escénico-Musicales de Puerto Rico y la Corporación de la Orquesta Sinfónica de Puerto Rico. La Corporación provee los servicios administrativos y el apoyo gerencial necesario a sus dos corporaciones subsidiarias y sus programas músico-sociales.

Los poderes de la Corporación son ejercidos por una Junta de Directores (Junta), cuyo propósito es establecer, dirigir, supervisar y llevar a cabo todos los programas relacionados con la cultura musical y las artes escénico-musicales. La Junta está compuesta por nueve miembros nombrados por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico. El Gobernador nombra al presidente de la Junta entre los miembros de la misma.

La administración y supervisión de las operaciones de la Corporación las ejerce un director ejecutivo nombrado por la Junta de Directores, con la aprobación del Gobernador. La estructura organizacional de la Corporación consiste en las oficinas de la directora ejecutiva, Finanzas, Recursos Humanos y Relaciones Laborales, Servicios Generales, y los Programas Músico-Sociales.

[2] Mediante la *Ley 141-1995*, se otorgó autonomía operacional y fiscal a la Corporación del Conservatorio de Música de Puerto Rico, por lo que dejó de ser una subsidiaria de la Corporación.

Al 25 de mayo de 2017, la oficina de la directora ejecutiva contaba con un oficial principal de informática que estaba a cargo de las operaciones de los sistemas de información computadorizados de la Corporación[3].

La Corporación cuenta con una red de comunicación de área local (*LAN*, por sus siglas en inglés) que interconecta los equipos ubicados en el Centro Gubernamental Roberto Sánchez Vilella y en la Sala Sinfónica de Puerto Rico. La Corporación utiliza un sistema financiero y un sistema de asistencia. Mediante estos sistemas, también provee los servicios de contabilidad y de procesamiento de la nómina a sus subsidiarias.

El presupuesto de la Corporación proviene de resoluciones conjuntas del presupuesto general, asignaciones especiales e ingresos propios. El presupuesto asignado para los años fiscales del 2015-16 al 2017-18 ascendió a $9,143,679, $9,519,610 y $8,812,060, 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.cam.pr.gov. Esta página provee información acerca de las actividades ofrecidas por la Corporación y sus subsidiarias, entre otros.

COMUNICACIÓN CON LA GERENCIA

El borrador de este *Informe* se remitió al Prof. Carlos Ruiz Cortés, director ejecutivo, para comentarios, por carta del 25 de enero de 2019. Con el mismo propósito, remitimos el borrador de los hallazgos este *Informe* a la Prof. Mercedes Gómez Marrero, exdirectora ejecutiva, por carta de la misma fecha.

[3] El oficial principal de informática tenía reservado en la Corporación el puesto de administrador de servidores, mientras ocupaba el puesto de confianza.

El 13 de marzo de 2019 la Lcda. Islaim Rodríguez Luna, subdirectora ejecutiva de la Corporación, contestó el borrador, en representación del director ejecutivo, y nos indicó, entre otras cosas, lo siguiente:

> Es necesario establecer que la administración actual y la Junta de Directores de la Corporaciones comenzaron sus funciones el pasado agosto de 2018. Siendo así que la nueva administración no tenía ningún conocimiento acerca de la auditoría que había sido efectuada. Los pasados administradores no informaron de la misma en la transición de la corporación. Advinimos a conocimiento de esta cuando nos fue entregado el borrador del informe. [*sic*]
>
> Durante este tiempo nos hemos dado a la tarea de buscar y/o levantar la información relacionada a los hallazgos mencionados en el borrador del informe. No obstante, a pesar de la búsqueda y ante la falta del personal técnico especializado en el área de sistemas de computadoras, no hemos encontrado información que nos ayude a emitir algún tipo de comentario preciso e informado para cada uno de los hallazgos. [*sic*]

La exdirectora ejecutiva contestó el 23 de febrero de 2019 el borrador de los hallazgos de este *Informe*. En los **hallazgos** se incluyeron algunos de sus comentarios.

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 los objetivos 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** de este *Informe* se comentan las deficiencias de controles internos significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado.

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 los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de los sistemas de información computadorizados 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 4** que se comentan a continuación.

Hallazgo 1 - Falta de un informe del análisis de riesgos de los sistemas de información computadorizados, de un procedimiento para el manejo de incidentes, y de un inventario de programas instalados en los servidores y las computadoras de la Corporación

Situaciones

a. El análisis de riesgos de los sistemas de información computadorizados es un proceso a través del cual se identifican los activos de 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 implantados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

Al 13 de julio de 2017, la Corporación no había preparado un informe de análisis de riesgos de los sistemas de información computadorizados.

b. Al 13 de julio de 2017, la Corporación no tenía un procedimiento o plan para el manejo de incidentes de seguridad que estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

c. Al 13 de julio de 2017, la Corporación no mantenía un inventario de los programas adquiridos e instalados en sus servidores y computadoras.

Criterios

Las situaciones comentadas se apartan de lo establecido en las políticas *ATI-003, Seguridad de los Sistemas de Información*; *ATI-015, Programa de Continuidad Gubernamental*; y *ATI-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*; de la *Carta Circular 140-16*.

Efectos

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

La situación comentada en el **apartado b.** le impide a la Corporación tener un control eficaz y documentado sobre el manejo de incidentes. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

La situación comentada en el **apartado c.** le impide a la Corporación ejercer un control eficaz de los programas computadorizados y sus licencias. Esto, a su vez, puede propiciar la instalación y el uso de programas no autorizados, sin que se puedan detectar a tiempo para fijar responsabilidades. Además, priva a la Corporación de información necesaria para la implementación de controles para protegerse de las amenazas a las que puedan estar expuestos estos programas.

Causa

Las situaciones comentadas se debieron, en parte, a que la Corporación solo contaba con el oficial principal de informática para atender los asuntos relacionados con los sistemas de información computadorizados. Esto, limitó el tiempo disponible para preparar el análisis de riesgos, el procedimiento para el manejo de incidentes y el inventario de los programas instalados en los servidores y las computadoras de la Corporación.

Comentarios de la Gerencia

La exdirectora ejecutiva de la Corporación nos indicó, entre otras cosas, las gestiones que inició durante su incumbencia para corregir la situación comentada en el **apartado c.** del **Hallazgo**.

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

Hallazgo 2 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Al 13 de julio de 2017, la Corporación carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de los sistemas de información

computadorizados. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la Corporación, en caso de riesgos como: virus de computadoras, ataques cibernéticos o desastres naturales, entre otros.

A la fecha de nuestro examen, la Corporación solo contaba con un borrador del *IT Disaster Recovery Plan (Plan)* que fue preparado en el 2015. Según informó el oficial principal de informática, este *Plan* no estaba actualizado.

b. Al 13 de julio de 2017, la Corporación no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*.

Lo comentado en el **apartado b.** es contrario a lo sugerido en el Capítulo 3.5, *Contingency Planning*, del *FISCAM*. En este se indica 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. En dichos convenios debe incluirse una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios.

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 e interrupciones prolongadas de los servicios a los usuarios de la Corporación.

Además, la situación comentada en el **apartado b.** podría afectar las operaciones de la Corporación y los servicios de los sistemas de información computadorizados, ya que no tendrían disponibles unas

instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de los archivos y el pronto restablecimiento de las operaciones normales de los sistemas de información computadorizados.

Causas

Las situaciones comentadas se debieron, en parte, a que la Corporación solo contaba con el oficial principal de informática para atender los asuntos relacionados con los sistemas de información computadorizados. Esto, limitó el tiempo disponible para preparar el plan de continuidad de negocios, y para identificar y establecer los acuerdos para un centro alterno. **[Apartados a. y b.]**

Además, 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-a.]**

Comentarios de la Gerencia

La exdirectora ejecutiva de la Corporación nos indicó, entre otras cosas, lo siguiente:

> […] dimos curso a la compra de un servidor […], para que fungiera de servidor alterno al ya existente. Dicho servidor fue ubicado temporeramente en […], con el compromiso de que, cuando nos entregaran la nueva sede […], dicho servidor sería instalado como servidor alterno […]. [*sic*]

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

Hallazgo 3 - Deficiencias en el almacenamiento y las pruebas de restauración de los respaldos de las bases de datos de los sistemas principales de la Corporación

Situaciones

a. El oficial principal de informática era responsable de preparar diariamente los respaldos de las bases de datos del sistema financiero y del sistema de asistencia. Estos respaldos eran producidos de forma automatizada mediante una aplicación y grabados en ocho discos internos del servidor de respaldo.

El examen realizado sobre los procedimientos utilizados para la producción y el almacenamiento de los respaldos reveló que, al 12 de junio de 2017, el oficial principal de informática:

1) No producía una copia adicional de los respaldos para mantenerla en un lugar seguro y distante del centro de procesamiento de datos.

2) No realizaba pruebas de restauración de los respaldos de las bases de datos. Esto, con el propósito de que la Corporación pudiera comprobar la efectividad de los respaldos realizados, y asegurar la recuperación exitosa de la información y la continuidad de sus operaciones, en caso de alguna eventualidad.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Capítulo 3.5, *Contingency Planning*, del *FISCAM*. En este se indica que las copias de la información que sean necesarias para mantener las operaciones deben mantenerse en lugares distantes de la entidad. Esto, con el propósito de que no estén expuestas a las mismas amenazas y estén disponibles en caso de una emergencia o desastre.**[Apartado a.1)]**

Además, establece que para determinar la efectividad de los planes de contingencia se deben realizar simulaciones de desastres que incluyan pruebas de restauración de los archivos y sistemas respaldados, en el lugar externo. **[Apartado a.2)]**

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)** podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales y afectar las funciones de la Corporación y sus sistemas de información computadorizados.

Causa

Las situaciones comentadas se debían a que la Corporación no contaba con un procedimiento aprobado que requiriera, entre otras cosas, el almacenamiento de los respaldos de información computadorizada en un lugar seguro y distante del centro de procesamiento de datos, y el efectuar pruebas de restauración de los mismos.

Comentarios de la Gerencia

La exdirectora ejecutiva de la Corporación nos indicó, entre otras cosas, las gestiones que inició durante su incumbencia para corregir las situaciones comentadas.

Véanse las recomendaciones 1 y 3.a.2).

Hallazgo 4 - Falta de un formulario para la creación, modificación y cancelación de las cuentas de acceso; y de una herramienta para generar informes relacionados con el tráfico de entrada y salida en Internet

Situaciones

a. Al 12 de junio de 2017, la Corporación no había establecido un formulario para la solicitud, aprobación, creación, modificación y cancelación de las cuentas de acceso de los usuarios para acceder a la red, y el uso de las aplicaciones, el correo electrónico e Internet. Las solicitudes se realizaban mediante comunicación verbal o por correo electrónico al oficial principal de informática.

b. La Corporación contaba con un cortafuego (*firewall)* que controlaba el tráfico de los paquetes de información durante la entrada y salida a Internet. Al 13 de julio de 2017, el oficial principal de informática no tenía disponible una herramienta que le permitiera generar los informes del cortafuego, necesarios para realizar las revisiones periódicas del tráfico de estos paquetes de información.

Criterios

Las situaciones comentadas son contrarias a la *Política ATI-003* de la *Carta Circular 140-16*. En esta se establece, entre otras cosas, que las entidades gubernamentales deben implementar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada.

Además, establece que:

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

- Deben existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten. **[Apartado b.]**

- Las agencias deben establecer los controles necesarios para evitar que, de forma intencionada o accidental, se inicien ataques desde sus redes internas hacia otros sistemas de información externos. **[Apartado b.]**

Además, la situación comentada en el **apartado a.** es contraria a lo establecido en el Capítulo 3.2, *Access Control*, del *FISCAM*. En este se indica que las autorizaciones de acceso deben ser documentadas en formularios y se deben mantener archivadas.

Efectos

La situación comentada en el **apartado a.** impide mantener la evidencia requerida de las autorizaciones para otorgar, modificar o cancelar los accesos y los privilegios a los usuarios. Esto dificulta las revisiones periódicas de las autorizaciones de acceso. Además, puede afectar la integridad de la información registrada en las aplicaciones de la Corporación.

La situación comentada en el **apartado b.** priva a la Corporación de bitácoras del tráfico de la red necesarias para detectar las violaciones de seguridad que puedan resultar en el daño a los equipos, y la pérdida o

divulgación no autorizada de la información mantenida en los sistemas computadorizados. Esto puede propiciar que las violaciones de seguridad no puedan ser detectadas a tiempo para fijar responsabilidades y tomar prontamente las medidas preventivas y correctivas necesarias.

Causas

La situación comentada en el **apartado a.** se debió, en parte, a la falta de un procedimiento para la administración y el control de las cuentas de acceso de la Corporación.

La situación comentada en el **apartado b.** se debió a que el paquete de servicios del cortafuego adquirido por la Corporación no incluía el acceso para generar informes de seguridad, y esto requería un costo adicional.

Comentarios de la Gerencia

La exdirectora ejecutiva de la Corporación nos indicó, entre otras cosas, las gestiones que inició durante su incumbencia para corregir la situación comentada en el **apartado a.** del **Hallazgo**.

Véanse las recomendaciones 1, y 3.a.3) y e.

RECOMENDACIONES

A la Junta de Directores de la Corporación de las Artes Musicales

1. Ver que el director ejecutivo cumpla con las **recomendaciones 2 y 3** de este *Informe*. **[Hallazgos del 1 al 4]**

Al director ejecutivo de la Corporación de las Artes Musicales

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

3. Ejercer una supervisión efectiva sobre el oficial principal de informática para asegurarse de que:

    a. Prepare y remita para su revisión, y la aprobación de la Junta, procedimientos para:

        1) El manejo de incidentes. Como parte de este procedimiento, debe requerirse que se mantenga la documentación de los incidentes y la metodología utilizada para resolverlos. Esto, de manera que, cuando estos se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información computadorizados y la continuidad de las operaciones. **[Hallazgo 1-b.]**

        2) La preparación, el almacenamiento y las pruebas de restauración de los respaldos. Este procedimiento debe requerir que se mantenga una copia de los respaldos de datos en un lugar seguro y distante del centro de procesamiento de datos de la Corporación, y que se realicen periódicamente las pruebas de restauración de estos. **[Hallazgo 3]**

        3) La administración y el control de las cuentas de acceso de la Corporación. Este procedimiento debe requerir el uso de un formulario para documentar las autorizaciones de acceso a los sistemas de información computadorizados de la Corporación. **[Hallazgo 4-a.]**

    b. Mantenga un registro de los programas adquiridos por la Corporación e instalados en sus servidores y computadoras. Este registro debe incluir, entre otra información, el número de la licencia y el costo del programa instalado; el nombre del usuario; el número de propiedad; y la descripción de la computadora donde está instalado el mismo. Esto, con el fin de mantener un inventario de dichos programas y detectar la instalación de los no autorizados. **[Hallazgo 1-c.]**

c. Actualice, complete y remita, para su revisión y la aprobación de la Junta, el plan de continuidad de negocios. Este debe incluir un plan para la recuperación de desastres y un plan para la continuidad de las operaciones, según se establece en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*. Una vez el documento sea revisado y aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro y distante 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.]**

d. Realice las gestiones necesarias para establecer un centro alterno, y se asegure de que el mismo cuente con el equipo necesario para restaurar las operaciones críticas de los sistemas de información computadorizados, en caso de desastres o emergencias. **[Hallazgo 2-b.]**

e. Identifique e implemente alternativas costo-efectivas para realizar revisiones periódicas del tráfico de los paquetes de información durante la entrada y salida a Internet. Una vez implementadas, realice revisiones periódicas del tráfico de la red y establezca las medidas preventivas y correctivas necesarias para mantener la seguridad de las conexiones en Internet. **[Hallazgo 4-b.]**

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 DE LAS ARTES MUSICALES
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. José A. Frontera Agenjo	Presidente Interino	1 ago. 17	26 ene. 18
Lcdo. Michel J. Godreau Robles	Presidente	1 may. 17	31 jul. 17
Sra. María Firpi Samper	Vicepresidenta[4]	1 may. 17	31 jul. 17

[4] Este puesto estuvo vacante del 1 de agosto de 2017 al 26 de enero de 2018.

ANEJO 2

CORPORACIÓN DE LAS ARTES MUSICALES
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Prof. Mercedes Gómez Marrero	Directora Ejecutiva	1 may. 17	26 ene. 18
Sr. Giovanni A. Bueno Orengo	Subdirector	1 may. 17	26 ene. 18
Sra. Iralda M. Abarca Alomía	Directora de Recursos Humanos y Relaciones Laborales[5]	22 may. 17	26 ene. 18
Sr. Xavier E. Cardona Jiménez	Oficial Principal de Informática[6]	1 may. 17	15 jul. 17

[5] El puesto estuvo vacante del 1 al 21 de mayo de 2017.

[6] Del 16 de julio de 2017 al 26 de enero de 2018, el oficial principal de informática se acogió a una licencia sin sueldo.

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-18-19* del 27 de abril de 2018, 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