12605

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

7193

RECIBIDO MAY21'18PM3:50
PRESIDENCIA DEL SENADO

21 de mayo de 2018

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

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

SECRETARÍA DEL SENADO
RECIBIDO MAY22 2018 AM10:13

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-18-10* de la Oficina de Sistemas de Información de la Corporación de Puerto Rico para la Difusión Pública, aprobado por esta Oficina el 15 de mayo de 2018. 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-18-10

15 de mayo de 2018

Corporación de Puerto Rico para la Difusión Pública

Oficina de Sistemas de Información

(Unidad 5213 - Auditoría 14067)

Período auditado: 30 de septiembre de 2015 al 15 de septiembre 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 **6**

CONTROL INTERNO **7**

OPINIÓN Y HALLAZGOS **8**

1 - Falta de un plan de continuidad de negocios, deficiencias relacionadas con el Plan de Contingencia para los sistemas de información computadorizados de la Corporación, y falta de un centro alterno 8

2 - Deficiencias relacionadas con los controles físicos en los cuartos de distribución de cableado 13

3 - Deficiencias relacionadas con los parámetros de seguridad y controles de acceso, y falta de revisiones periódicas de los registros de eventos de los sistemas operativos de los servidores 16

4 - Deficiencias relacionadas con el manejo, control y almacenamiento de los respaldos de información, y falta de pruebas de restauración de los mismos 19

5 - Falta de documentación de la justificación y autorización de los accesos a las cuentas con privilegios de conexión remota 23

COMENTARIO ESPECIAL **24**

Deficiencia en el cómputo de retención en el origen de la contribución sobre ingresos de los empleados de la Corporación 24

RECOMENDACIONES **24**

APROBACIÓN **27**

ANEJO 1 - INFORME PUBLICADO **28**

ANEJO 2 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **29**

ANEJO 3 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **30**

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

15 de mayo 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 la Oficina de Sistemas de Información (OSI) de la Corporación de Puerto Rico para la Difusión Pública (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 para la continuidad del servicio; el acceso lógico a las redes de comunicación y a la aplicación *Sage Fund Accounting* (*Sage MIP*); y la documentación, la entrada, el procesamiento y la salida de los datos de dicha aplicación, 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 segundo y último informe, y contiene cinco hallazgos y un Comentario Especial del resultado del examen que realizamos de lo indicado en la sección anterior. En el **ANEJO 1** presentamos información sobre el primer informe emitido relacionado con las operaciones de la OSI de la Corporación. Estos están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 30 de septiembre de 2015 al 15 de septiembre 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 a funcionarios, empleados y contratistas; inspecciones físicas; exámenes 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

La Corporación se creó mediante la *Ley Núm. 7 del 2 de enero de 1987*, en la cual se facultó a la Autoridad de Teléfonos de Puerto Rico a crear una subsidiaria sin fines pecuniarios denominada Corporación de Puerto Rico para la Difusión Pública. Mediante dicha *Ley* se transfirieron a la Corporación las instalaciones de radio y televisión del Departamento de Instrucción Pública (ahora Departamento de Educación)[1]. La Corporación desarrollaría y operaría dichas instalaciones para fines educativos, culturales y de interés público.

Posteriormente, mediante la *Ley 216-1996*, según enmendada, se creó una nueva corporación, con el mismo nombre, pero independiente de la Autoridad de Teléfonos de Puerto Rico. Esto, con el propósito de garantizar unos servicios de excelencia cónsonos con el desarrollo social, tecnológico y económico de nuestra sociedad.

En dicha *Ley* se dispone que la Corporación funciona como entidad independiente separada de cualquier otra dependencia del Gobierno del

[1] Los servicios de radio y televisión del Gobierno bajo la jurisdicción del referido Departamento se conocían como WIPR y fueron administrados por este hasta el 30 de junio de 1988. A partir de esta fecha, la Corporación administra los mencionados servicios.

Estado Libre Asociado de Puerto Rico, dirigida por una junta de directores (Junta) compuesta por 13 miembros[2]. Estos son el secretario de Educación, el presidente de la Universidad de Puerto Rico, el director ejecutivo del Instituto de Cultura Puertorriqueña, el secretario de Recreación y Deportes, el director ejecutivo de la Compañía de Fomento Industrial de Puerto Rico, y 8 ciudadanos provenientes del sector privado, quienes son nombrados por el Gobernador con el consentimiento del Senado de Puerto Rico. Por lo menos, 3 de estos ciudadanos deben ser personas de comprobado interés, conocimiento y experiencia en educación, cultura, artes, ciencias o comunicaciones de radio y televisión. La Junta elige al presidente, al vicepresidente, quien sustituye al presidente en su ausencia, y al secretario. Además, elige entre sus miembros al presidente de la Corporación. La Junta tiene la facultad para aprobar, enmendar y derogar aquellos reglamentos que estimen necesarios o convenientes para llevar a cabo sus fines, propósitos y actividades.

Las funciones administrativas de la Corporación son ejercidas por el presidente, quien es responsable, ante la Junta, de la ejecución de la política que esta establezca y de la supervisión general de todos los funcionarios, empleados y agentes de la Corporación. En la *Ley 216-1996* se dispone que el presidente de la Corporación es miembro de la Junta, pero no tiene derecho al voto ni puede ocupar ningún cargo oficial.

La estructura organizacional de la Corporación está compuesta por las oficinas de Presidencia, Asuntos Legales, Auditoría Interna[3], Mercadeo y Relaciones Públicas, y Planificación y Desarrollo; y los departamentos de Administración[4], Ingeniería, Programación, Producción y Radio.

---

[2] La *Ley 216-1996* fue enmendada por la *Ley 88-2014* para aumentar de 11 a 13 los miembros que componen la Junta.

[3] La Oficina de Auditoría Interna le responde funcionalmente al Comité de Auditoría y a la Junta de Directores de la Corporación. El director de esta Oficina le responde a la presidenta para propósitos administrativos.

[4] El Departamento de Administración está compuesto por las oficinas de Servicios Administrativos, de Finanzas y Presupuesto, y de Recursos Humanos.

A la fecha de nuestra auditoría, la OSI estaba adscrita al Departamento de Ingeniería, y era dirigida por el vicepresidente de ingeniería[5], quien respondía directamente a la presidenta. La OSI contaba con tres contratistas externos que realizaban funciones de especialista en informática, técnico de computadoras y coordinadora de aplicaciones, y una empleada regular que ocupaba el puesto de recepcionista. El puesto de director de sistemas de información estaba vacante desde junio de 2013.

La Corporación ofrece sus servicios de transmisión a través de 8 antenas instaladas en 7 torres localizadas alrededor de Puerto Rico y la infraestructura tecnológica de la Corporación actualmente consiste de:

- Una red de comunicación de área local para comunicar los servidores y las computadoras en las instalaciones de Hato Rey
- Una red de comunicación con Mayagüez mediante *Multiprotocol Label Switching* (*MPLS*)[6]
- Diez servidores conectados a la red localizados en la OSI de la Corporación
- Ciento cincuenta y cinco computadoras de escritorio, y 4 computadoras portátiles
- Doscientas cuarenta y seis cuentas de acceso asignadas a usuarios y 28 cuentas asignadas a varios servicios.

[5] El 20 de noviembre de 2013 el Ing. Jorge González Fonseca fue nombrado por la presidenta de la Corporación como vicepresidente de ingeniería y, desde esa fecha, tenía a cargo la supervisión de la OSI y del Área de Master Control. El ingeniero González Fonseca renunció el 31 de agosto de 2016, y fue sustituido por el Sr. Christian O. Medina Morales, gerente de ingeniería interino.

[6] Mecanismo de transporte de datos que opera entre la capa de enlace de datos y la capa de enlace de la red del modelo de interconexión de sistemas abiertos. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizada para transportar tráfico de voz y paquetes de Protocolo de Internet (IP, por sus siglas en inglés).

Para cumplir con su misión, la Corporación cuenta con tres aplicaciones que fueron desarrolladas por contratistas externos. Estas son:

- *Protrack* - Maneja la información del contenido de las estaciones de televisión y genera el itinerario diario de la programación a transmitirse.
- *Sage MIP* - Permite el registro de las transacciones de contabilidad, las adquisiciones, el presupuesto, la nómina y los recursos humanos, entre otros.
- *Microix* - Genera las requisiciones de bienes y servicios, y las órdenes de compra.

Los recursos para financiar las actividades operacionales de la Corporación provienen de la Resolución Conjunta del Presupuesto General, asignaciones especiales, fondos especiales estatales y federales e ingresos propios. Los gastos operacionales de la OSI son sufragados del presupuesto operacional de la Corporación que, para los años fiscales del 2014-15 al 2016-17, ascendió a $17,397,000, $16,168,999 y $15,735,000, respectivamente.

Los **anejos 2 y 3** 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.wipr.pr. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* y otras situaciones determinadas durante la auditoría, fueron remitidas a la Lcda. Cecille M. Blondet Passalacqua, entonces presidenta de la Corporación, mediante cartas de nuestros auditores del 18 de mayo y 4 de noviembre de 2016. En las referidas cartas se incluyeron detalles sobre las situaciones comentadas.

Mediante cartas del 6 de junio y 1 diciembre de 2016, la licenciada Blondet Passalacqua contestó las cartas de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

Mediante cartas del 20 de marzo de 2018, se remitió, para comentarios, el borrador de este *Informe* al Dr. Rafael Batista Cruz, presidente de la Corporación; y el borrador de los **hallazgos** a la licenciada Blondet Passalacqua, expresidenta.

El presidente contestó el borrador mediante carta del 4 de abril e indicó, entre otras cosas, lo siguiente:

> Desde que asumí la encomienda de dirigir la Corporación en el año 2017, he estado enfocado junto a mi equipo de trabajo en atender con urgencia todos los asuntos recomendados por su oficina durante los pasados años. Actualmente, respondemos todas las recomendaciones hechas durante la primera auditoría y ahora, en esta segunda fase, trabajaremos con la misma responsabilidad corrigiendo todos los asuntos señalados. Es importante resaltar que muchas de las recomendaciones ya se atendieron o están siendo corregidas conforme a las instrucciones de la Oficina del Contralor. [*sic*]
>
> He dado instrucciones a todos los departamentos y personal a cargo de las áreas auditadas, para que todos estos procesos se realicen de acuerdo a los requerimientos de ley y exigencias de su oficina. Una vez publicado el informe, le estaremos remitiendo toda la documentación requerida y con toda la responsabilidad que siempre nos ha caracterizado. [*sic*]

El 4 de abril de 2018 la licenciada Blondet Passalacqua solicitó una prórroga para remitir sus comentarios, la cual le concedimos hasta el 16 de abril de 2018. La licenciada Blondet Passalacqua contestó el borrador mediante carta de ese mismo día. 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 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** 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.

Las deficiencias comentadas no constituyen necesariamente todos los aspectos de control interno que pudieron 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 5** que se comentan a continuación.

Hallazgo 1 - Falta de un plan de continuidad de negocios, deficiencias relacionadas con el Plan de Contingencia para los sistemas de información computadorizados de la Corporación, y falta de un centro alterno

Situaciones

a. Al 17 de noviembre de 2015, la Corporación no contaba con un plan de continuidad de negocios que incluyera los planes específicos completos y actualizados de la OSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información

computadorizados y restaurar las operaciones de la Corporación en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red de comunicación o desastres naturales, entre otros.

b. El examen del *Plan de Contingencia* de la Corporación, que nos fue provisto el 3 de diciembre de 2015, reveló las siguientes deficiencias:

1) No estaba aprobado por el presidente de la Junta de la Corporación.

2) No incluía los siguientes requisitos para atender situaciones de emergencia:

- Los procedimientos a seguir cuando la OSI no puede recibir ni transmitir información de los usuarios que acceden los sistemas de información mediante conexiones remotas
- El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones, y archivos críticos del área de sistemas de información
- La documentación actualizada de la infraestructura de la red y de los procesos de respaldo
- Un itinerario de restauración que incluyera el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
- El detalle de la configuración de los equipos críticos (equipo de comunicación y servidores), del contenido de los respaldos, y de los archivos
- El nombre del encargado de activar el plan y del personal de reserva, recuperación, emergencias y seguridad, de forma tal que pueda ser ejecutado sin depender de individuos específicos

- Una lista de los números de teléfonos de los miembros de cada grupo de recuperación y de los proveedores de servicios y aplicaciones
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

c. Al 17 de noviembre de 2015, la Corporación no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en caso de emergencia.

Situaciones similares a las de los **apartados b. y c.** fueron comentadas en el *Informe de Auditoría TI-02-11* del 7 de mayo de 2002.

Criterios

La situación comentada en el **apartado a.** es contraria a 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 de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la directora de la Oficina de Gerencia y Presupuesto (OGP); y en la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el director de la OGP[7].

La situación comentada en el **apartado b.** es contraria a lo establecido en el *Manual de Normas y Procedimientos para la Administración, Seguridad y Uso de los Sistemas de Información* (*Manual de Normas*), aprobado el 20 de marzo de 2003 por el presidente de la Junta. En este se dispone que la OSI deberá coordinar y establecer planes de contingencia para las aplicaciones críticas de la Corporación.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que, como parte del plan de

[7] 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.

continuidad de negocios, se debe preparar un plan de contingencias. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presenten eventualidades inesperadas que afecten su funcionamiento. El mismo debe estar aprobado por el funcionario de máxima autoridad de la entidad y debe incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado b.]**

Además, dichas prácticas sugieren que, como parte integral del plan de continuidad de negocios, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la entidad, podrían ser los siguientes: **[Apartado c.]**

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

Efectos

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

La situación comentada en el **apartado c.** podría afectar las funciones de la OSI y los servicios 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 retrasar o impedir el proceso

de restauración de archivos y el pronto restablecimiento de las operaciones normales de los sistemas de información computadorizados de la Corporación.

Causas

Las situaciones comentadas en los **apartados a. y b.** se debieron al desconocimiento que tenía el personal de la OSI de los requerimientos específicos necesarios para la preparación de los planes de continuidad de negocio y de contingencias.

La situación comentada en el **apartado c.** se debió a limitaciones presupuestarias de la Corporación, y a que la OSI no tenía una partida de presupuesto asignada para los sistemas de información computadorizados.

Comentarios de la Gerencia

La expresidenta indicó, entre otras cosas, las gestiones que comenzó a realizar antes de su renuncia, para corregir las situaciones comentadas en los **apartados a., b.1) y c.**

Además, con relación al **apartado b.2)**, indicó, entre otras cosas, lo siguiente:

> […] al momento de la auditoría la Corporación sí contaba con un Plan de Contingencia para Situaciones de Emergencia por escrito que incluía la protección del equipo y acceso a los datos en caso de desastres naturales, incluyendo la ejecución de tareas administrativas de compras y pagos en situaciones de emergencia. Además, la Corporación tomaba medidas para evitar daños a sus equipos por variaciones de voltajes, contaba con programas antivirus instalados en sus computadoras, y requería contraseñas y establecía jerarquías de seguridad para acceso a la red y sistemas. [*sic*]

Consideramos las alegaciones de la expresidenta con respecto al **apartado b.2)**, pero determinamos que el mismo prevalece. Esto, debido a que el plan al que hace referencia es distinto al entregado para examen, y tampoco contemplaba los sistemas de información computadorizados ni los procesos para asegurar la continuidad de los procesos de la OSI.

Véanse las recomendaciones 2, 3.a. y b., y 4.

Hallazgo 2 - Deficiencias relacionadas con los controles físicos en los cuartos de distribución de cableado

Situaciones

a. La Corporación contaba con 3 cuartos de distribución de cableado, de los cuales, 2 se encontraban localizados en el edificio principal y 1 en el edificio de Administración. Los 3 cuartos tenían instalado un *switch*[8], que interconectaba las computadoras que recibían servicio de la red.

En el examen realizado el 9 de agosto de 2016 relacionado con los controles físicos[9] existentes en dichos cuartos, se identificaron las siguientes deficiencias:

1) Los cables de transmisión de los concentradores de los tres cuartos no estaban organizados ni identificados. Esto es necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones.

2) En los tres cuartos no había un diagrama esquemático que ilustrara las conexiones establecidas con los equipos.

3) En uno de los cuartos, además del equipo de comunicación, se mantenía el panel de los cables del servicio telefónico, y en otro se mantenía el ponchador de asistencias del área de Administración. Esto dificulta mantener un control de acceso adecuado a dichos cuartos.

Situaciones similares fueron comentadas en el *Informe de Auditoría TI-02-11*.

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 cada agencia es responsable de desarrollar políticas específicas de seguridad de

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

[9] Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

acuerdo con las características propias de sus ambientes de tecnología, particularmente sus sistemas críticos. Esto implica que, como norma de sana administración, las agencias deben tener los cuidados necesarios para proteger los equipos computadorizados contra daños y averías, y para mantener el funcionamiento óptimo de los mismos. Para garantizar razonablemente la seguridad de los equipos y de los sistemas computadorizados, es necesario que:

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada. **[Apartado a.1) y 2)]**

- Se controle adecuadamente el acceso a las áreas donde están ubicados los equipos de comunicación. **[Apartado a.3)]**

Las situaciones comentadas en el **apartado a.1) y 2)** también se apartan de lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de dicha *Carta Circular*. En esta se establece que las entidades gubernamentales tienen la responsabilidad de adquirir e implementar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientes. Además, se establece que las redes en las entidades deben proveer la infraestructura necesaria para implementar y mantener los procesos de negocio de la entidad gubernamental, y ser operacionales y confiables.

Lo comentado en el **apartado a.2) y 3)** se aparta de lo establecido en el *Manual de Normas*, en el que se dispone, entre otras cosas, lo siguiente:

- La OSI es responsable de mantener los diagramas de configuración de la red de una manera clara y precisa, así como un inventario de los equipos existentes. **[Apartado a.2)]**

- El único personal autorizado a entrar al área de los servidores y del equipo de telecomunicación es el que labora en la OSI. **[Apartado a.3)]**

Efectos

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

La situación comentada en el **apartado a.3)** puede propiciar que personas no autorizadas y ajenas a la OSI, por error o intencionalmente, causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y la divulgación indebida de información, dificulta la adjudicación de responsabilidades a las personas que comentan estos actos, y podría afectar adversamente el funcionamiento de la red y la continuidad de las operaciones.

Causas

Las situaciones comentadas se debieron a que el vicepresidente de ingeniería no veló por que el especialista en informática:

- Estableciera los controles de seguridad físicos adecuados para proteger el equipo de comunicación de la Corporación y sus respectivas conexiones **[Apartado a.]**
- Cumpliera con las disposiciones establecidas en el *Manual de Normas*. **[Apartado a.2) y 3)]**

Comentarios de la Gerencia

La expresidenta indicó, entre otras cosas, las gestiones que comenzó a realizar, antes de su renuncia para mantener un control de acceso adecuado a los cuartos de cableado examinados. **[Apartado a.3)]**

Véanse las recomendaciones 2 y 3.d.

Hallazgo 3 - Deficiencias relacionadas con los parámetros de seguridad y controles de acceso, y falta de revisiones periódicas de los registros de eventos de los sistemas operativos de los servidores

Situaciones

a. La OSI contaba con un servidor principal mediante el cual se controlaba el acceso a los recursos de la red. El examen efectuado el 24 de mayo de 2016 sobre los parámetros de seguridad establecidos en el sistema operativo de este servidor reveló que no se había definido lo siguiente:

    1) Las políticas relacionadas con las contraseñas (*password policy*) para requerir:

        a) Al menos, tres contraseñas diferentes antes de repetir una utilizada anteriormente (*enforce password history*).

        b) Un mínimo de días para que el sistema le requiera al usuario cambiar la contraseña nuevamente (*minimum password age*).

        c) Un máximo de días para que el sistema le requiera al usuario cambiar la contraseña nuevamente (*maximum password age*).

        d) La utilización de contraseñas complejas (*password must meet complexity requirements*).

    2) Las políticas de seguridad para restringir el tiempo de acceso a la red para todas las cuentas, de acuerdo con las funciones de cada usuario (*disconnect clients when logon expire*).

b. Al 24 de noviembre de 2015, el especialista en informática, quien era responsable de administrar la red, no examinaba periódicamente los registros de eventos y violaciones de seguridad provistos por el sistema operativo. Esto, 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. Solamente se verificaban los registros del *firewall*[10] y del correo electrónico.

Una situación similar a la del **apartado a.** fue comentada en el *Informe de Auditoría TI-03-10* del 12 de mayo de 2003.

Criterios

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

- El uso de todas las opciones para restringir y controlar los accesos que proveen distintos sistemas operativos. **[Apartado a.]**
- La limitación del tiempo de acceso para todas las cuentas de acuerdo con las funciones de cada usuario **[Apartado a.2)]**
- El examen continuo de los informes que detallan los eventos inusuales del sistema. **[Apartado b.]**

Además, la situación comentada en el **apartado a.** es contraria a lo establecido en el *Manual de Normas*. En este se establece, entre otras cosas, lo siguiente:

- El sistema mantendrá un historial de las últimas tres contraseñas utilizadas. **[Apartado a.1)a)]**
- Se seleccionará una contraseña que tenga, al menos, cinco caracteres alfanuméricos, y que incluya una combinación de letras mayúsculas y minúsculas, números y símbolos. **[Apartado a.1)d)]**

[10] Sistema que se coloca entre una red de comunicación e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad y autentificación, entre otros.

Efectos

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

Lo comentado en el **apartado b.** impide a la Corporación mantener un registro de los eventos inusuales o problemas ocurridos en la red que le permita al especialista en informática tomar a tiempo las medidas correctivas o preventivas necesarias. Además, impide la detección temprana de errores críticos o problemas en los servidores y en las computadoras, de acceso no autorizados y del uso indebido de los sistemas.

Causa

Las situaciones comentadas se debían a que el vicepresidente de ingeniería no le había impartido las instrucciones al especialista en informática para poner en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo, y para revisar periódicamente los registros de los eventos de seguridad que provee el sistema operativo.

Comentarios de la Gerencia

La expresidenta indicó, entre otras cosas, lo siguiente:

> […] Señala el Informe que no existe una política definida sobre las contraseñas de los usuarios, sin embargo en la práctica sí existen parámetros para las contraseñas que menciona el Informe por lo que no estamos de acuerdo con dicho hallazgo. Por ejemplo, las normas y sistemas ya requerían contraseñas de acceso a la red con un mínimo de seis dígitos o más. Los mismos pueden ser numéricos o alfanuméricos. De igual forma toda contraseña tenía término de expiración. Por lo que entendemos que las normas establecidas cumplen con las necesidades de la Corporación. [*sic*] **[Apartado a.]**

> […] No estamos de acuerdo con dicho hallazgo, toda vez que según comunicamos en la carta de 1ro de diciembre de 2016, el Especialista sí verificaba los eventos o intentos de violaciones de seguridad en el sistema. De hecho el "firewall" da aviso de dichos eventos y los mismos se verificaban diariamente. […] [*sic*] **[Apartado b.]**

Consideramos las alegaciones de la expresidenta con respecto a los **apartados a. y b.**, pero determinamos que los mismos prevalecen. Esto, debido a lo siguiente:

- La evidencia recopilada por nuestros auditores, a la fecha de nuestra auditoría, mostraba que las políticas de contraseñas indicadas no estaban definidas. Además, en la contestación del presidente, no se nos indicó ni se nos suministró evidencia de que en la Corporación se hubieran definido dichas políticas.

- Los eventos que se recopilan en los registros de los sistemas operativos no incluyen los que se mantienen en los registros del *firewall*. Este último se relaciona con los eventos de accesos internos y externos a las redes e Internet.

Véanse las recomendaciones 2 y 3.e.

Hallazgo 4 - Deficiencias relacionadas con el manejo, control y almacenamiento de los respaldos de información, y falta de pruebas de restauración de los mismos

Situaciones

a. La Corporación contaba con 10 servidores conectados a la red, los cuales estaban localizados en la OSI. Diariamente se le realizaban respaldos automáticos a los 4 servidores que mantenían la información de las aplicaciones *Sage MIP* y *Microix*, del correo electrónico, de la página en Internet, y de los documentos guardados por los usuarios de la Corporación. Estos respaldos se generaban de forma incremental, con excepción de los viernes que eran realizados de manera completa (*full backup*), y se mantenían en el servidor de los respaldos.

El contratista externo que realizaba las funciones de técnico de computadoras producía los días 15 y 30 de cada mes, los respaldos de la información mantenida en los servidores, y los grababa en una cinta magnética. Al próximo día laborable guardaba la cinta en la caja de seguridad de la Oficina de Finanzas y Presupuesto. De esta manera, se sustituía la cinta más reciente por la que estaba guardada y que correspondía a la quincena anterior.

La información de la cinta era registrada en el *Application Server Backup Log* (*Backup Log*). En este se incluía la fecha y hora en que se realizó el respaldo, el número de cinta en que se grabó, las iniciales de quien lo preparó y los comentarios para indicar si se completó la grabación del respaldo en cinta.

El examen efectuado sobre el manejo, control y almacenamiento de los respaldos de información, al 20 de octubre de 2015, reveló lo siguiente:

1) No se mantenían copias de los respaldos en un lugar seguro fuera de los predios de la Corporación. La Oficina de Finanzas y Presupuesto, en la que se mantenían dichos respaldos, estaba ubicada en el edificio contiguo al principal de la Corporación, por lo que estaba expuesto a las mismas amenazas.

2) El *Backup Log* no proveía información sobre el contenido de los respaldos almacenados ni del servidor al que pertenecían.

b. Al 20 de octubre de 2015, no se realizaban pruebas periódicas de restauración de los respaldos de la información mantenida en estos servidores. Esto, para verificar que se pudiera recuperar la información en caso de una falla en el sistema o el equipo.

Una situación similar al **apartado a.1)** fue comentada en el *Informe de Auditoría TI-02-11*.

Criterios

Las situaciones comentadas en el **apartado a.** son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades deben mantener una copia de respaldo recurrente de la información de los programas de aplicación y de sistemas esenciales e importantes, para las operaciones de la Corporación. En consonancia con dicha *Política*, es necesario, entre otras cosas, que las entidades gubernamentales se aseguren de que:

- Toda la 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 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. **[Apartado a.1)]**

- Se mantenga un inventario detallado de las cintas de respaldos para facilitar su localización y sustituirlas periódicamente, y para documentar el cumplimiento de las normas y los procedimientos establecidos. **[Apartado a.2)]**

La situación comentada en el **apartado a.1)**, además, es contraria a lo establecido en el *Manual de Normas*. En el mismo se establece, entre otras cosas, que toda la información almacenada en medios electrónicos que se utilice como parte de la operación normal de la Corporación debe ser duplicada diariamente y guardada en un lugar seguro fuera de los predios de la Corporación. Además, se debe mantener en bóveda, por un año, el respaldo que corresponde al día 30 de cada mes.

Las mejores prácticas en el campo de la tecnología de información sugieren que los respaldos de información se remitan a pruebas periódicas de restauración. Esto es necesario para garantizar la continuidad de las operaciones en caso de que ocurra un evento inesperado en las instalaciones de la Corporación. **[Apartado b.]**

Efectos

La situación comentada en el **apartado a.1)** puede ocasionar que, en casos de emergencias, la Corporación no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Lo comentado en el **apartado a.2)** priva a la Corporación de un control adecuado sobre los respaldos realizados y almacenados en el servidor, y dificulta la localización e identificación del contenido de los mismos.

La situación comentada en el **apartado b.** representa un alto riesgo para la Corporación de incurrir en interrupciones prolongadas, en caso de que el respaldo realizado no pueda ser restaurado exitosamente, luego de ocurrir alguna eventualidad.

Causa

Las situaciones comentadas se atribuyen a que el vicepresidente de ingeniería de la OSI no había desarrollado un procedimiento para la preparación, el manejo y el almacenamiento de los respaldos para asegurarse de que el técnico de computadoras:

- Cumpliera con lo establecido en el *Manual de Normas* **[Apartado a.1)]**
- Incluyera, en el *Backup Log*, la información sobre el contenido de los respaldos preparados y el servidor al que pertenece la misma **[Apartado a.2)]**
- Realizara pruebas periódicas de restauración a los respaldos de información de la Corporación. **[Apartado b.]**

Comentarios de la Gerencia

La expresidenta nos indicó, entre otras cosas, lo siguiente:

> […] a la luz de las recomendaciones de la auditoría a diciembre de 2016 se evaluaba con los consultores que preparaban el Plan de Continuidad la posibilidad de realizar los resguardos en nube. […] [*sic*] **[Apartado a.1)]**

Véanse las recomendaciones 2 y 3.c.

Hallazgo 5 - Falta de documentación de la justificación y autorización de los accesos a las cuentas con privilegios de conexión remota

Situación

a. No se encontró, ni le fue suministrado a nuestros auditores, evidencia de que se hubiera autorizado el privilegio de conexión remota para 13 usuarios de la red. Este tipo de privilegio permite acceder y utilizar la información computadorizada de una entidad gubernamental desde un lugar remoto o distinto de donde está guardada la misma.

Criterios

La situación comentada se aparta de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades gubernamentales deben implementar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada. Además, se establece que si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deben existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. Para cumplir con esta *Política*, se deben establecer normas y procedimientos específicos para la asignación del privilegio de acceso remoto a los usuarios, donde se incluya, entre otras cosas, la justificación y autorización para el otorgamiento de dichos privilegios.

Efectos

La situación comentada impide mantener un control de los usuarios autorizados a acceder los sistemas de información computadorizados y de los privilegios asignados a estos para fijar responsabilidades en caso de errores o irregularidades. Esto, a su vez, puede propiciar que personas no autorizadas puedan lograr el acceso a información confidencial y hacer uso indebido de esta.

Causa

Lo comentado se debió a que el vicepresidente de ingeniería no veló por que el especialista en informática incluyera, en el *Manual de Normas*, directrices que permitieran documentar la justificación y autorización de las cuentas con privilegios de conexión remota a los sistemas computadorizados de la Corporación.

Comentarios de la Gerencia

La expresidenta indicó, entre otras cosas, lo siguiente:

> […] se estableció el proceso para que toda solicitud de acceso a la red o de conexión remota se documentara […].

Véanse las recomendaciones 2 y 3.f.

COMENTARIO ESPECIAL

En esta sección se comentan situaciones que no necesariamente implican violaciones de leyes y de reglamentos, pero que son significativas para las operaciones de la entidad auditada. También se incluyen situaciones que no están directamente relacionadas con las operaciones de la entidad, las cuales pueden constituir violaciones de leyes o de reglamentos, que afectan al erario.

Deficiencia en el cómputo de retención en el origen de la contribución sobre ingresos de los empleados de la Corporación

Situación

Durante nuestra auditoría detectamos una situación relacionada con la retención de contribuciones sobre ingresos, realizada a los empleados de la Corporación. La misma fue referida al secretario de Hacienda, para su análisis y consideración, mediante carta del 25 de abril de 2018 **(RTI-5213-14067-18-01)**.

Véase la Recomendación 1.

RECOMENDACIONES

Al Secretario de Hacienda

1. Dar seguimiento a la situación referida por nuestra Oficina mediante carta del 25 de abril de 2018 **(RTI-5213-14067-18-01)**. **[Comentario Especial]**

A la Junta de Directores de la Corporación de Puerto Rico para la Difusión Pública

2. Ver que el presidente de la Corporación cumpla con las **recomendaciones 3 y 4**, de manera que se corrijan y no se repitan las situaciones comentadas en este *Informe*. **[Hallazgos del 1 al 5]**

Al Presidente de la Corporación de Puerto Rico para la Difusión Pública

3. Ejercer una supervisión efectiva sobre el vicepresidente de ingeniería, para asegurarse de que se:

    a. Identifiquen alternativas costo-efectivas para preparar un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan de continuidad de operaciones, de acuerdo con lo establecido en las políticas *ATI-003, Seguridad de los Sistemas de Información*, y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*. Una vez dicho plan sea revisado y aprobado, vele por que se realicen pruebas periódicas y se divulgue a los empleados y a los funcionarios concernientes. Además, se asegure de que se mantenga una copia actualizada del mismo en un lugar seguro fuera de los predios de la Corporación. **[Hallazgo 1-a.]**

    b. Actualice el *Plan de Contingencia* para que incluya los aspectos comentados en el **Hallazgo 1-b.**

    c. Prepare un procedimiento detallado sobre la preparación, el manejo y el almacenamiento de los respaldos de la información mantenida en los servidores. Entre otros aspectos, este procedimiento deberá considerar:

        1) El envío de una copia de los respaldos a un lugar externo fuera de los predios de la Corporación. **[Hallazgo 4.a.1)]**

        2) El registro en el *Backup Log*, de la información de los respaldos realizados y de los enviados a un lugar

externo. Entre la información registrada debe incluirse el contenido de los respaldos, y el servidor al que pertenecen los mismos. **[Hallazgo 4-a.2)]**

3) La realización de pruebas periódicas de restauración de los respaldos guardados en cinta magnética y almacenada en la caja de seguridad de la Oficina de Finanzas y Presupuesto. Esto, para comprobar la efectividad de los mismos. **[Hallazgo 4-b.]**

d. Impartan instrucciones al contratista externo, responsable de administrar la seguridad de los sistemas de información de la Corporación, para que:

1) Establezca las medidas y los controles necesarios para corregir las situaciones indicadas en el **Hallazgo 2**. Esto, de manera que se asegure de que los equipos de comunicación de la Corporación estén protegidos contra posibles accesos no autorizados, que puedan afectar la confidencialidad de la información y la disponibilidad y el rendimiento de estos equipos.

2) Prepare un diagrama esquemático de la red de comunicación de la Corporación que incluya la interconexión de los equipos (servidores, *switches*, *firewall*, entre otros), la descripción del equipo y su configuración básica (modelo, nombre, *IP Address*), y el sistema operativo de las computadoras conectadas a la red. Además, asegurarse de que el mismo se mantenga actualizado. **[Hallazgo 2-a.2)]**

e. Efectúen las modificaciones en los parámetros de seguridad del sistema operativo del servidor principal de la red para:

1) Restringir a los usuarios el poder repetir las últimas tres contraseñas utilizadas **[Hallazgo 3-a.1)a)]**

2) Establecer un término para que las contraseñas de las cuentas de acceso expiren, y requerir a los usuarios cambiar periódicamente las mismas. **[Hallazgo 3-a.1)b) y c)]**

3) Requerir a los usuarios la utilización de contraseñas complejas. **[Hallazgo 3-a.1)d)]**

4) Desactivar automáticamente del sistema a los usuarios una vez venza el término de acceso a la red establecido. **[Hallazgo 3-a.2)]**

5) Revisar periódicamente el registro de eventos que produce el servidor principal y los intentos de acceso a la red de la Corporación y, de ser necesario, implementar de inmediato las medidas correctivas que correspondan. **[Hallazgo 3-b.]**

f. Impartan instrucciones al especialista en informática para que incluya, en el *Manual de Normas*, directrices para requerir que, para cada cuenta con privilegio de conexión remota otorgada, se documente la justificación y la autorización correspondiente. **[Hallazgo 5]**

4. Realizar las gestiones necesarias para que la Corporación cuente con un centro alterno para la recuperación de las operaciones computadorizadas. **[Hallazgo 1-c.]**

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 PUERTO RICO PARA LA DIFUSIÓN PÚBLICA
OFICINA DE SISTEMAS DE INFORMACIÓN

INFORME PUBLICADO

INFORME	FECHA	CONTENIDO DEL INFORME
TI-17-06	24 ene. 17	Resultado del examen de los controles internos establecidos para la administración de la seguridad y la función de la Oficina de Auditoría Interna de la Corporación.

ANEJO 2

CORPORACIÓN DE PUERTO RICO PARA LA DIFUSIÓN PÚBLICA
OFICINA DE SISTEMAS DE INFORMACIÓN

MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Braulio Castillo Quintero	Presidente[11]	14 sep. 16	15 sep. 16
Lcdo. Armando Valdés Prieto	"	30 sep. 15	15 may. 16
Lcdo. Álex López Echegaray	Vicepresidente	14 sep. 16	15 sep. 16
Sr. Braulio Castillo Quintero	"	30 sep. 15	13 sep. 16
Sr. Rafael E. Irizarry Cuebas	Secretario	30 sep. 15	15 sep. 16

[11] Este puesto estuvo vacante desde el 16 de mayo hasta el 13 de septiembre de 2016.

ANEJO 3

CORPORACIÓN DE PUERTO RICO PARA LA DIFUSIÓN PÚBLICA
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcda. Cecille M. Blondet Passalacqua	Presidenta	30 sep. 15	15 sep. 16
Sr. Víctor Rivera Rodríguez	Vicepresidente de Administración y Recursos Humanos	30 sep. 15	15 sep. 16
Ing. Jorge E. González Fonseca	Vicepresidente de Ingeniería[12]	30 sep. 15	31 ago. 16
Sr. Daniel Villanueva Mercado	Director de Finanzas y Presupuesto	30 sep. 15	15 sep. 16

[12] Véase la nota al calce 5.

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