INFORME DE AUDITORÍA TI-17-06

24 de enero de 2017

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 3 de febrero de 2016

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **6**

OPINIÓN Y HALLAZGOS **6**

1 - Falta de un informe de análisis de riesgos y de un análisis de impacto de negocio sobre los sistemas de información 7

2 - Falta de un plan escrito para el manejo de incidentes y de adiestramientos al Vicepresidente de Ingeniería sobre la seguridad de los sistemas de información 9

3 - Falta de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados, y disposiciones no incluidas en el Manual de Normas 11

4 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y las operaciones de los sistemas de información computadorizados de la Corporación 14

RECOMENDACIONES **15**

AGRADECIMIENTO **17**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **18**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **19**

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

24 de enero de 2017

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

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 30 de septiembre de 2015 al 3 de febrero de 2016. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; 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.

CONTENIDO DEL INFORME

Este es el primer informe, y contiene cuatro hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración de la seguridad y la función de la Oficina de Auditoría Interna de la Corporación. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

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 funcionará como una entidad independiente separada de cualquier otra dependencia del Gobierno del 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 serán nombrados por el Gobernador con el consentimiento del Senado de Puerto Rico. Por lo menos, 3 de estos ciudadanos deberán 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.

[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.

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

Además, elige entre sus miembros al Presidente de la Corporación. La Junta tiene la facultad para aprobar, enmendar y derogar aquellos reglamentos que estime necesarios o convenientes para llevar a cabo sus fines, propósitos y actividades.

Las funciones administrativas de la Corporación son ejercidas por su 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 podrá 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.

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 2013.

[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.

[5] El 20 de noviembre de 2013 el Ing. Jorge González Fonseca fue nombrado por la Presidenta 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.

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 la tecnología *Multiprotocol Label Switching* (*MPLS*)[6]
- Diez servidores conectados a la red corporativa localizados en la OSI de la Corporación
- Ciento cincuenta y cinco computadoras de escritorio y cuatro computadoras portátiles
- Doscientas cuarenta y seis cuentas de acceso asignadas a usuarios y veintiocho cuentas asignadas a varios servicios.

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 Fund Accounting (Sage MIP)* - Permite el registro de las transacciones de contabilidad, de las adquisiciones, del presupuesto, de la nómina y de 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 2013-14 al 2015-16 ascendió a $18,131,000, $17,397,000 y 16,168,999, respectivamente.

[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).

Los **anejos 1 y 2** contienen una relación de los miembros de la Junta de Directores 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, relacionadas con los controles internos establecidos para la administración del programa de seguridad y la función de la Oficina de Auditoría Interna de la Corporación, fueron remitidas a la Lcda. Cecille M. Blondet Passalacqua, entonces Presidenta de la Corporación, mediante carta de nuestros auditores del 18 de mayo de 2016. En la referida carta se incluyeron detalles sobre las situaciones comentadas.

Mediante carta del 6 de junio de 2016, la entonces Presidenta remitió sus comentarios, los cuales fueron considerados en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió para comentarios a la licenciada Blondet Passalacqua, por carta del 28 de octubre de 2016. El 14 de noviembre solicitó una prórroga para remitir sus comentarios, la cual le concedimos hasta el 21 de noviembre.

La entonces Presidenta de la Corporación contestó el borrador mediante carta del 21 de noviembre. Sus comentarios fueron considerados en la redacción final de este *Informe* y en los **hallazgos** se incluyen algunos de sus comentarios.

OPINIÓN Y HALLAZGOS

Opinión favorable con excepciones

Las pruebas efectuadas demostraron que las operaciones de la OSI, en lo que concierne a los controles establecidos para la administración de la seguridad de los sistemas de información computadorizados de la

Corporación, se realizaron sustancialmente de acuerdo con las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 4** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos y de un análisis de impacto de negocio sobre los sistemas de información

Situaciones

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 la 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 cerciora de 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 28 de octubre de 2015, en la Corporación no se había preparado un informe de análisis de riesgos de los sistemas de información computadorizados.

b. El análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por la pérdida o interrupción de las operaciones, y de las vulnerabilidades y amenazas que fueron identificadas y clasificadas en el análisis de riesgos. Además, debe proveer información para determinar las estrategias de recuperación más apropiadas. Al 28 de octubre de 2015, en la Corporación no se había realizado un análisis de impacto de negocio sobre los sistemas de información computadorizados.

Criterios

Las situaciones comentadas son contrarias 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[7], aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto (OGP).

Además, son contrarias a lo establecido en la *Política TIG-015, Programa de Continuidad Gubernamental,* aprobada el 22 de septiembre de 2011 por el Director de la OGP.

Efectos

Las situaciones comentadas impiden a la Corporación estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y de pérdida de información. Además, dificultan 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 alguna eventualidad.

Causas

Las situaciones comentadas se debieron principalmente al desconocimiento de quien dirigía la OSI de la Corporación, sobre la importancia de preparar el análisis de riesgos y el análisis de impacto de negocio, y de los requerimientos específicos para la preparación de estos informes. Además, la Corporación no había preparado los análisis mencionados debido a la falta de presupuesto y de personal capacitado.

La situación comentada en el **apartado b.** se atribuye a que la Corporación desconocía que debía incluir a la OSI en el análisis de impacto de negocio realizado a la entidad.

Comentarios de la Gerencia

La entonces Presidenta nos indicó en su carta, entre otras cosas, que, conscientes de la importancia que tienen las redes de comunicación y los servidores de la Corporación para sus operaciones, han contratado una firma para que, antes de que finalice el 2016, complete el análisis de riesgos y

[7] Dicha *Carta Circular* fue derogada 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* derogada.

prepare el plan de acción comprensivo. Este incluirá normas, políticas, procedimientos y estrategias para que el personal pueda utilizarlo como referencia al momento de atender cualquier riesgo o desastre que afecte los sistemas de la Corporación.

Véanse las recomendaciones 1 y 3.

Hallazgo 2 - Falta de un plan escrito para el manejo de incidentes y de adiestramientos al Vicepresidente de Ingeniería sobre la seguridad de los sistemas de información

Situaciones

a. Al 17 de noviembre de 2015, la OSI no tenía un procedimiento o plan para el manejo de incidentes en el que se 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.

b. El 20 de noviembre de 2013 la entonces Presidenta nombró al Vicepresidente de Ingeniería para, entre otras cosas, estar a cargo de la supervisión de la OSI, la cual contaba con tres contratistas externos. Estos contratistas estaban encargados de la administración de los sistemas de información computadorizados, los servicios técnicos y el desarrollo de la página en Internet de la Corporación.

   En la hoja de deberes y la descripción del puesto del Vicepresidente de Ingeniería[8], no se incluían funciones relacionadas con la administración y supervisión de los sistemas de información computadorizados. Además, su experiencia era en el área de ingeniería y no en la de sistemas de información.

   Al 25 de noviembre de 2015, el Vicepresidente de Ingeniería no había recibido adiestramientos relacionados con la seguridad de los sistemas de información computadorizados. Estos adiestramientos eran necesarios para que este funcionario pudiera ejercer las tareas relacionadas con la administración de los sistemas computadorizados de la Corporación, y la supervisión del personal contratado en la OSI.

[8] En la hoja de deberes el nombre de este puesto era Jefe de Ingeniería y en la descripción del puesto era Director de Ingeniería.

Esto, para lograr el buen funcionamiento de los sistemas de información, las redes de comunicación y la página en Internet de la Corporación.

Criterios

Las situaciones comentadas son contrarias a lo establecido en las políticas *TIG-003* y *TIG-015* de la *Carta Circular 77-05*.

La situación comentada en el **apartado b.** es contraria a lo establecido en el Artículo IX del *Reglamento para la Administración de los Recursos Humanos del Servicio de Confianza Gerencial de la Corporación de Puerto Rico para la Difusión Pública*, aprobado el 29 de junio de 2004 y enmendado el 10 de diciembre de 2004 por el Presidente de la Junta de Directores de la Corporación. En este se establece que, en la medida que los recursos disponibles lo permitan, la Corporación proveerá a los empleados de confianza los instrumentos necesarios para la capacitación y el desarrollo de destrezas para lograr una mayor productividad y calidad en los servicios. Además, el Presidente podrá hacer extensivo a los empleados de confianza los beneficios sobre las actividades de adiestramientos que se disponen en el Artículo 10 del *Reglamento para la Administración de los Recursos Humanos del Servicio de Carrera Gerencial de la Corporación*.

Efectos

La situación comentada en el **apartado a.** impide a la OSI 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 b.** podría afectar las operaciones de la OSI y la seguridad de los sistemas de información de la Corporación. Además, priva al Vicepresidente de Ingeniería de los conocimientos necesarios que le permitan asegurar el establecimiento de los controles de seguridad necesarios para proteger los sistemas de información computadorizados de la Corporación, y supervisar efectivamente al personal contratado por la OSI.

Causas

La situación comentada en el **apartado a.** se atribuye a que el personal de la OSI no tenía el conocimiento para desarrollar el plan para el manejo de incidentes. Además, se debía a las limitaciones de presupuesto existentes en la Corporación.

La situación comentada en el **apartado b.** se debió a que el Vicepresidente de Administración y Recursos Humanos no veló por que se efectuaran estudios sobre las necesidades de capacitación y desarrollo de los recursos humanos para preparar programas y actividades de adiestramientos. Esto, con el propósito de proveer al Vicepresidente de Ingeniería los conocimientos relacionados con el manejo de la seguridad de los sistemas de información.

Comentarios de la Gerencia

La entonces Presidenta nos indicó en su carta, entre otras cosas, las medidas que están en proceso para corregir la situación comentada en el **apartado a.** del **Hallazgo**. Además, nos indicó lo siguiente:

> […] la Oficina de Recursos Humanos de la Corporación inquirió a OCALARH, la Universidad de Puerto Rico, y la Oficina de Gerencia y Presupuesto la disponibilidad de ofrecimiento de adiestramientos sobre seguridad de los sistemas de información. Y se nos informó que ellos no tienen este tipo de adiestramiento. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1, 4.a.1) y 5.

Hallazgo 3 - Falta de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados, y disposiciones no incluidas en el Manual de Normas

Situaciones

a. A la fecha de nuestro examen, en la Corporación no se habían promulgado procedimientos escritos para reglamentar lo siguiente:

   - La administración y el control de los accesos lógicos y físicos de los recursos de tecnología de información
   - El otorgamiento, la modificación o la cancelación del acceso local y remoto a los usuarios
   - La identificación, selección, instalación y modificación del sistema operativo de las computadoras

- La instalación y configuración de la red de comunicaciones
- El mantenimiento al equipo, y la administración y documentación de los problemas y los cambios, de manera que se prevengan las interrupciones no esperadas
- La preparación y el almacenamiento de los respaldos de información
- La adquisición de aplicaciones computadorizadas y el control de los cambios a las mismas.

b. La Corporación contaba con 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 de Directores. El propósito del *Manual de Normas* era establecer una política para el uso y manejo de los sistemas de información de la Corporación. El *Manual de Normas* incluye los estándares mínimos que debe seguir todo el personal o persona contratada que tenga acceso a los sistemas de información de la Corporación.

En el examen realizado el 10 de noviembre de 2015 al *Manual de Normas*, determinamos que no establecía disposiciones para lo siguiente:

- Reservar el derecho de decodificar documentos, establecer la forma y autorización necesaria para la instalación de programas, e instruir sobre la ubicación de los archivos que se crean en las computadoras para que puedan protegerse mediante los mecanismos de respaldo establecidos por la entidad.
- Prohibir el cambio de los parámetros de configuración de comunicación de equipos sin autorización y el uso de medios de almacenaje de información no certificados libre de virus.
- Prohibir el uso de las computadoras y el sistema de correo electrónico para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas o religiosas, u origen social o nacional, o que puedan ser

catalogados como hostigamiento sexual. Además, prohibir la divulgación de opiniones sobre personas con impedimento físico o mental.

- Prohibir el uso de protectores de monitores que puedan resultar poco serios u ofensivos.

Criterio

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05.* En esta se establece que será responsabilidad de cada entidad desarrollar normas específicas que consideren las características propias de los ambientes de tecnología, particularmente, sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer las políticas, las normas y los procedimientos escritos de control interno eficaces y actualizados que reglamenten las operaciones computadorizadas y que estén aprobadas por la alta gerencia. Mediante estos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia, y facilitan el adiestramiento.

Efectos

La situación comentada en el **apartado a.** podría ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias.

La situación comentada en el **apartado b.** le impide a la Corporación mantener controles adecuados para el uso de sus sistemas de información computadorizados, y podría exponer la información a riesgos innecesarios. Además, esta situación podría promover el uso indebido de los sistemas de información computadorizados y dificultar la imposición de sanciones en caso de que ocurra alguna irregularidad.

Causa

Las situaciones comentadas se atribuyen a la limitación de recursos existentes en la Corporación para adoptar y actualizar las normas y los procedimientos escritos para las operaciones de los sistemas de información computadorizados.

Comentarios de la Gerencia

La entonces presidenta nos indicó en su carta, entre otras cosas, las medidas implementadas y las que están en proceso para corregir la situación comentada en el **apartado b.**

Véanse las recomendaciones 1, y 4.a.2) y b.

Hallazgo 4 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y las operaciones de los sistemas de información computadorizados de la Corporación

Situación

a. La Corporación cuenta con la Oficina de Auditora Interna, la cual responde al Comité de Auditoría de la Junta de Directores. Dicha Oficina tiene como objetivo examinar los controles establecidos y sus sistemas de información computadorizados, con el propósito de asesorar y hacer recomendaciones al Presidente y a la Junta de Directores de la Corporación.

   El examen realizado reveló que, desde el 1 de julio de 2006, en la Corporación no se habían realizado evaluaciones o auditorías relacionadas con los procedimientos, los controles y las operaciones de los sistemas de información computadorizados.

Criterio

En las normas para la práctica profesional de la auditoría interna se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y evaluación de las exposiciones a los riesgos, y contribuir al mejoramiento de los sistemas de gestión de riesgos y control. También se establece que la actividad de auditoría interna debe evaluar las exposiciones de riesgo referidas al gobierno, las operaciones y los sistemas de información de la organización, con relación a lo siguiente:

- La confiabilidad e integridad de la información financiera y operativa

- La eficacia y eficiencia de las operaciones
- La protección de activos
- El cumplimiento de leyes, regulaciones y contratos.

Efectos

La falta de evaluaciones o auditorías relacionadas con los procedimientos, los controles y las operaciones de los sistemas de información computadorizados puede propiciar que se comentan errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades. También priva a la gerencia de información necesaria sobre el funcionamiento de los sistemas, los controles y las demás operaciones de la Corporación. Además, existe la posibilidad de que, en los sistemas de información, no se incluyan los controles básicos necesarios para evitar incurrir en errores, irregularidades y otras situaciones adversas.

Causas

La situación comentada se debe principalmente a la falta de personal especializado para realizar evaluaciones o auditorías de los sistemas de información computadorizados. Además, la Auditora Interna no había contemplado realizar este tipo de auditoría.

Comentarios de la Gerencia

La entonces Presidenta nos indicó en su carta, entre otras cosas, lo siguiente:

> Dada la especialización que requiere una auditoría de sistemas de información y que la Oficina de Auditoría Interna de la Corporación está compuesta por una sola persona, se le solicitó a la Auditora Interna que junto al Vicepresidente de Administración identifiquen recursos externos que se puedan contratar para colaborar con su oficina a realizar dicha tarea. [*sic*]

Véanse las recomendaciones 1 y 2.

RECOMENDACIONES

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

1. Ver que la Presidenta de la Corporación cumpla con las **recomendaciones de la 3 a la 5** de este *Informe*. **[Hallazgos del 1 al 3]**

2. Ver que la Auditora Interna realice las gestiones necesarias para que se efectúen auditorías relacionadas con los procedimientos, los controles y las operaciones de los sistemas de información computadorizados de la Corporación. **[Hallazgo 4]**

A la Presidenta de la Corporación de Puerto Rico para la Difusión Pública

3. Asegurarse de que se realicen y se documenten los análisis de riesgos de los sistemas de información computadorizados y de impacto de negocios, según se establecen en las políticas *TIG-003* y *TIG-015*. Los mismos deben ser remitidos para su revisión y para la aprobación de la Junta. Una vez aprobados, ver que los mismos se revisen cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de la Corporación para asegurarse de que se mantengan actualizados. **[Hallazgo 1]**

4. Ejercer una supervisión efectiva sobre el Gerente de Ingeniería Interino para asegurarse de que:

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

        1) El procedimiento para el manejo de incidentes. Como parte de este, debe requerirse que se documenten todos los incidentes y se indique cómo se resolvieron. Esto, de manera que, cuando dichos incidentes se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información computadorizados y la continuidad de las operaciones. **[Hallazgo 2-a.]**

        2) Las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 3-a.**

    b. Enmiende y remita para su revisión, y la aprobación de la Junta el *Manual de Normas*, para incluir las disposiciones sobre el uso de los sistemas de información computadorizadas indicadas en el **Hallazgo 3-b.**

5. Ejercer una supervisión eficaz sobre el Vicepresidente de Administración y Recursos Humanos para asegurarse de que se realice un estudio sobre las necesidades de adiestramientos de los funcionarios

y de los empleados que tengan a su cargo la seguridad de los sistemas de información computadorizados. Además, vele por que se ofrezcan dichos adiestramientos para corregir la situación mencionada en el **Hallazgo 2-b.** En cuanto a las personas contratadas, velar por que estos mantengan actualizados sus conocimientos relacionados con la seguridad de los sistemas de información computadorizados.

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmín M. Valdivieso

ANEJO 1

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
Lcdo. Armando Valdés Prieto	Presidente	30 sep. 15	3 feb. 16
Sr. Braulio Castillo Quintero	Vicepresidente	30 sep. 15	3 feb. 16
Sr. Rafael E. Irizarry Cuebas	Secretario	30 sep. 15	3 feb. 16

ANEJO 2

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	3 feb. 16
Sr. Víctor Rivera Rodríguez	Vicepresidente de Administración y Recursos Humanos	30 sep. 15	3 feb. 16
Ing. Jorge E. González Fonseca	Vicepresidente de Ingeniería	30 sep. 15	3 feb. 16
Sra. Sonia Vázquez Ibáñez	Auditora Interna	30 sep. 15	3 feb. 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, extensión 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