#12277

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

6257

PRESIDENCIA DEL SENADO

RECIBIDO ABR 3'18 PM 4:34

MTVC

Yesmín M. Valdivieso
Contralora

3 de abril de 2018

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

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

SECRETARIA DEL SENADO

SECRETARIA DEL SENADO
RECIBIDO ABR04 2018 PM 6:14

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-18-05* de la Oficina de Sistemas de Información del Cuerpo de Emergencias Médicas del Estado Libre Asociado de Puerto Rico, aprobado por esta Oficina el 20 de marzo 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-18-05

20 de marzo de 2018

Cuerpo de Emergencias Médicas del Estado Libre Asociado de Puerto Rico

(Ahora Negociado del Cuerpo de Emergencias Médicas de Puerto Rico)

Oficina de Sistemas de Información

(Unidad 5225 - Auditoría 14055)

Período auditado: 24 de agosto de 2015 al 24 de junio de 2016

CONTENIDO

Página

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

20 de marzo de 2018

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos de las operaciones de la Oficina de Sistemas de Información (OSI) del Cuerpo de Emergencias Médicas del Estado Libre Asociado de Puerto Rico (CEM). 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 del CEM, en lo que concierne a los controles internos para la administración de la seguridad, el acceso lógico y la continuidad del servicio, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 24 de agosto de 2015 al 24 de junio de 2016. El examen lo efectuamos de acuerdo a 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 entidad auditada o por fuentes externas; pruebas y análisis de procedimientos de control interno, y de otros procesos; y confirmaciones de información pertinente.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

Mediante la *Ley 539-2004, Ley del Cuerpo de Emergencias Médicas del Estado Libre Asociado de Puerto Rico*, se creó el CEM, adscrito al Departamento de Salud, con autonomía fiscal y administrativa.

El CEM se creó con el fin de garantizarle a los ciudadanos un servicio de óptima calidad cuando, de forma no prevista, la condición de salud de estos necesite cuidado médico prehospitalario, transportación a una instalación médico-hospitalaria adecuada, o primeros auxilios para preservar su salud o disminuir un daño o incapacidad permanente, que pueda surgir como consecuencia de una enfermedad o un accidente. Para prestar este servicio, el CEM contaba con 11 zonas y 60 ubicaciones[1] a través de toda la isla, las cuales disponían de ambulancias equipadas con equipos de emergencia.

A la fecha de nuestra auditoría, el CEM era dirigido por una directora ejecutiva, nombrada por el Gobernador de Puerto Rico. La estructura organizacional del CEM contaba con las oficinas de Finanzas y Presupuesto; Administración; Asuntos Internos y Responsabilidad Profesional; Recursos Humanos y Relaciones Laborables; y Sistemas de Información, y las áreas Operacionales y de Despacho de Comunicaciones.

La OSI le respondía a la directora ejecutiva y tenía 1 directora de tecnología de información, 1 especialista en tecnología de sistemas de información y 1 técnico de sistemas de información. La OSI contaba con una red de área local (LAN, por sus siglas en inglés) compuesta

[1] Localidades en donde se encontraban ubicadas las ambulancias. Algunas de estas localidades tenían computadoras, y equipos de comunicación y multifuncional.

por 10 servidores, en la que se mantenían los datos y las aplicaciones utilizadas por el personal del CEM. La Oficina de Gerencia y Presupuesto (OGP) le proveía al CEM los servicios de correo electrónico e Internet.

El presupuesto asignado al CEM provenía de resoluciones conjuntas del presupuesto general, de fondos especiales estatales, y de otros ingresos. Estos últimos provenían de la facturación de los planes médicos. Los gastos operacionales de la OSI eran sufragados por el presupuesto operacional del CEM que, para los años fiscales del 2012-13 al 2014-15, asendió a $36,616,000, $36,361,000 y $35,098,000, respectivamente.

El 10 de abril de 2017 se aprobó la *Ley 20-2017, Ley del Departamento de Seguridad Pública de Puerto Rico*, la cual derogó la *Ley 539-2004*. Dicha *Ley* creó el Departamento de Seguridad Pública y el Negociado del Cuerpo de Emergencias Médicas de Puerto Rico (Negociado), el cual está adscrito al Departamento con los mismos objetivos del CEM. El Gobernador de Puerto Rico delegó la administración y supervisión inmediata del Negociado al secretario de Seguridad Pública y, para dirigir las operaciones diarias, creó el cargo de comisionado del Negociado del Cuerpo de Emergencias Médicas (comisionado).

El **ANEJO** contiene una relación de los funcionarios principales del CEM que actuaron durante el período auditado.

El Negociado cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.cempr.pr.gov. Esta página provee información acerca de la entidad y de los servicios que presta.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe*, y otra situación determinada durante la auditoría, fueron remitidas a la Dra. Rosana Otaño López, entonces directora ejecutiva del CEM, mediante carta de nuestros auditores del 8 de junio de 2016. En la referida carta se incluyeron detalles sobre las situaciones comentadas.

Mediante carta del 20 de junio, la doctora Otaño López contestó la carta de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

Mediante cartas del 6 de febrero de 2018, se remitió, para comentarios, el borrador de este *Informe* al Hon. Héctor M. Pesquera López, secretario de Seguridad Pública, y al Lcdo. Guillermo Torruella Farinacci, comisionado; y el borrador de los **hallazgos** a la doctora Otaño López, exdirectora ejecutiva del CEM.

El 16 de febrero de 2018 el secretario solicitó una prórroga para remitir sus comentarios y los del comisionado, la cual concedimos hasta el 1 de marzo. El secretario contestó el borrador mediante cartas del 22 de febrero y 1 de marzo, e indicó las medidas que están en proceso para corregir las situaciones comentadas en este *Informe*. Además, indicó lo siguiente:

> Entre las funciones administrativas del DSP está el requisito de establecer procedimientos y mecanismos para asegurar el intercambio seguro y eficiente de información entre los componentes del Departamento y con otras agencias. Al momento, nos encontramos en proceso de definir y establecer políticas y procesos internos para configurar y administrar los sistemas y aplicativos de manejo de información electrónica para todos los componentes. Como parte de esta integración, el DSP velará por el cumplimiento con las normas establecidas por nuestro gobierno para el manejo seguro de los sistemas de informática; inclusive de las mejores prácticas de la industria. En este proceso resolveremos en su totalidad los señalamientos hechos por su Agencia y expresados en el borrador del reporte de auditoria de la OSI, CEM. [*sic*]

El comisionado contestó el borrador mediante carta del 6 de marzo e indicó que se reafirmaba en lo establecido por el secretario en su comunicación. Además, indicó lo siguiente:

> Es importante destacar, que es compromiso del NCEM y por consiguiente del DSP cumplimentar todas las recomendaciones contenidas en el borrador del informe referido de forma que se tomen las medidas correctivas necesarias para que no se repitan prospectivamente. [*sic*]

La doctora Otaño López contestó mediante carta del 21 de febrero e indicó, entre otras cosas, lo siguiente:

> Actualmente no estoy en la agencia como es de su conocimiento. Mi incumbencia fue desde 15 de diciembre del 2014 hasta el 2 de enero del 2017, pero como ex servidora pública tengo una

> responsabilidad y deber que cumplir. Por este motivo me comunique con […] la Ex Directora de la Oficina de Sistemas de Información del CEM, para de esta forma corroborar si dichos hallazgos se habían solucionado. [*sic*]
>
> La […] me indicó que el CEM y su nuevo Director Ejecutivo contestaron dichos hallazgos, pero serán enviados al […] Comisionado del Departamento de Seguridad para su revisión y luego ser enviado a la Oficina del Contralor. De la misma forma discutí los hallazgos con la […] luego que ella tuvo la autorización del nuevo Director del CEM. [*sic*]

CONTROL INTERNO

La gerencia del CEM era 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 del CEM.

En los **hallazgos** de este *Informe* se comentan las deficiencias de control interno significativas, dentro del contexto del objetivo 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 la OSI del CEM, en lo que concierne a los controles objeto de este *Informe*, se realizaron 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 de análisis de riesgos sobre los sistemas de información computadorizados

Situación

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en una entidad, sus vulnerabilidades y las amenazas a las que se encuentran expuestos, así como 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 asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

   El CEM mantenía sus operaciones en forma computadorizada mediante el uso de la aplicación *NorthStar Computer Aided Dispatch* (CAD), la cual era utilizada para administrar el proceso de prestación de servicios médicos de emergencia. Además, mantenía otros sistemas para realizar sus funciones administrativas, tales como: *e-Roc*, para el procesamiento de las requisiciones y órdenes de compra; y *Kronos*, para el registro de la asistencia del personal. El CEM también contaba con 177 computadoras, y 10 servidores y equipos de comunicación, que eran parte de su red de área local mediante la cual se comunicaban las oficinas regionales y ubicaciones.

Estas aplicaciones, computadoras, servidores y equipos de comunicación formaban parte de los activos de sistemas de información computadorizados existentes en el CEM. Sin embargo, al 30 de septiembre de 2015, en el CEM no se había preparado el informe de análisis de riesgos de los sistemas de información computadorizados.

Criterios

La situación comentada 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 OGP. Además, es contraria 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[2].

Efecto

La situación comentada impidió al CEM estimar el impacto que los elementos de riesgos tuvieron sobre las áreas y los sistemas críticos de este, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Causa

La situación comentada se atribuyó a que la entonces directora ejecutiva no promulgó una directriz para la preparación y documentación de un análisis de riesgos, que incluyera todos los activos de sistemas de información del CEM.

Véanse las recomendaciones 1 y 2.

[2] 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.

Hallazgo 2 - Deficiencias relacionadas con los planes de continuidad de negocio, y de respuesta de emergencias y recuperación; y falta de un centro alterno para recuperar las operaciones administrativas computadorizadas y de un acuerdo escrito para restaurar la aplicación CAD en las instalaciones de la AEMEAD

Situaciones

a. El examen efectuado el 22 de septiembre de 2015 al *Continuity of Operations/Continuity of Government Plan* (*Plan*), revisado el 29 de diciembre de 2010, reveló las siguientes deficiencias:

   1) El *Plan* no se aprobó ni se actualizó. En el mismo se mencionaba a una compañía externa que no era la que proveía el servicio de mantenimiento a la aplicación CAD. Además, mencionaba incorrectamente los puestos de los empleados de la OSI.

   2) No contaba con un itinerario de restauración que incluyera el orden de prioridad de las aplicaciones a restaurar.

b. El examen efectuado el 22 de septiembre de 2015 al *Plan de Respuesta de Emergencias y Recuperación*, revisado el 19 de junio de 2013 por el director ejecutivo interino, reveló que no estaba actualizado. El mismo hacía referencia a compañías que no proveían servicios en el CEM.

c. Al 22 de septiembre de 2015, el CEM no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en caso de emergencia.

d. El CEM acordó verbalmente con la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico (AEMEAD)[3], establecer un centro alterno en sus instalaciones para, en caso de una emergencia, restaurar la aplicación CAD. Sin embargo, este acuerdo no se formalizó por escrito.

[3] Mediante la *Ley 20-2017*, la AEMEAD se integró al Departamento como el Negociado de Manejo de Emergencias y Administración de Desastres.

Criterios

Las situaciones comentadas en los **apartados a. y b.** son contrarias a lo establecido en la *Política TIG-015*.

La situación comentada en el **apartado b.** es contraria a lo establecido en el Inciso c. de la Sección: Respaldo de la Información, de las *Normas y Procedimientos de Seguridad y Uso de los Sistemas de Información*, aprobadas el 18 de diciembre de 2009 por el director ejecutivo. En estas se dispone que el director de informática deberá recomendar, para la aprobación del director ejecutivo, un plan de recuperación de desastres que servirá como guía para asegurar la restauración de los servicios computadorizados definidos como críticos, luego de situaciones en que estos se hayan perdido o destruido. Además, este se debe asegurar de que se implementen las acciones necesarias para actualizar el *Plan* cuando sea necesario y que el mismo se conserve actualizado en un lugar seguro fuera de los predios del CEM.

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

- Una entidad pública o privada de similar configuración 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.** pudieron propiciar la improvisación y, que en casos de emergencia, se tomaran medidas inapropiadas y sin orden alguno. Esto representó un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, y de interrupciones prolongadas de los servicios ofrecidos a los usuarios del CEM.

Las situaciones comentadas en los **apartados c. y d.** pudieron afectar las operaciones del CEM y los servicios de la OSI, ya que no tuvieron disponibles unas instalaciones para operar después de que una emergencia o de un evento afectara su funcionamiento. Esto pudo atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la OSI.

Causas

Las situaciones comentadas en los **apartados a. y b.** se atribuyeron a que la directora ejecutiva del CEM no impartió instrucciones a la directora de tecnología de información para que se asegurara de que se actualizara el *Plan* y lo remitiera para su aprobación.

La situación comentada en el **apartado c.** se debió a que, aunque la directora de tecnología de información identificó las instalaciones que utilizarían para establecer el centro alterno de las operaciones administrativas computadorizadas del CEM, no se configuraron los equipos que se utilizarían en el mismo.

La situación comentada en el **apartado d.** se debió a que la directora ejecutiva del CEM no requirió que se formalizara el acuerdo escrito con el director de la AEMEAD para utilizar los equipos y las instalaciones, en caso de alguna emergencia, para restaurar la aplicación CAD.

Véanse las recomendaciones 1, 3 de la a. a la c. y 4.

Hallazgo 3 - Falta de un formulario para solicitar cuentas de acceso y de un proceso de notificación del traslado o la separación del personal

Situaciones

a. El examen efectuado sobre el proceso de solicitud de acceso a los sistemas de información del CEM reveló que al 14 de marzo de 2016, no se utilizó un formulario para documentar la solicitud, aprobación creación, modificación y cancelación de las cuentas de los usuarios. Además, no se nos suministró evidencia de que se utilizaron correos electrónicos para solicitar y aprobar estas cuentas.

b. No existió un proceso para notificar a la OSI el traslado y la separación del personal con acceso a los sistemas de información del CEM. Esto, con el fin de asegurar que se efectuaran los cambios correspondientes en los privilegios de acceso que tenía este personal o se revocaran inmediatamente las cuentas de acceso.

Criterio

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

- Las entidades gubernamentales deberán implementar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada.

- La información y los programas de aplicación utilizados en las operaciones de la agencia deberán 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. Estos controles deberán incluir mecanismos de autenticación y autorización.

- Cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que

incluyan una comunicación efectiva entre el área de recursos humanos, el área en que trabaja el empleado, y el área de sistemas de información.

Esta norma se establece, en parte, mediante lo siguiente:

- El establecimiento de controles de acceso rigurosos a los programas y archivos, incluido el uso de formularios o de algún otro documento para solicitar y autorizar la creación de los accesos.
- El uso de formularios de autorización (en papel o electrónicos) en los que se establezca quién debe tener acceso a qué, y deben evidenciar la aprobación a nivel gerencial.
- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente.

Efectos

Las situaciones comentadas pudieron propiciar que personas no autorizadas accedieran información confidencial y la utilizaran indebidamente. Además, propiciaron la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que se detectaran a tiempo para fijar responsabilidades.

La situación comentada en el **apartado a.** impidió mantener la evidencia requerida para otorgar, modificar o cancelar los accesos y privilegios a los usuarios.

Causas

Las situaciones comentadas se atribuyeron a que el CEM no contaba con un procedimiento escrito para:

- Mantener documentada la solicitud, autorización, modificación y cancelación de las cuentas de acceso a las aplicaciones y los sistemas de información. **[Apartado a.]**

- Informar a la OSI el traslado o la separación del personal que tiene acceso a los sistemas de información computadorizados para la cancelación o modificación de las cuentas de acceso. **[Apartado b.]**

Véanse las recomendaciones 1, 3.d. y 5.

Hallazgo 4 - Falta de un registro y documentación relacionada con el seguimiento, el análisis y la solución de incidentes de seguridad en los sistemas de información

Situación

a. El 31 de julio de 2015 el CEM contrató a una compañía externa para administrar la red y la seguridad de los sistemas de información computadorizados. Como parte de sus responsabilidades, el personal de la compañía revisaba continua o periódicamente los equipos en la red, tales como: servidores, *switches*[4], *Gateway*, *DVR*[5] y el *Firewall*[6]. Para esto, utilizaba la aplicación *PRTG Network Monitor*. Una vez se detectaba una anomalía o incidente de seguridad, la aplicación enviaba avisos a través del correo electrónico a la directora de tecnología de información, al especialista en tecnología de sistemas de información y al personal de la compañía *externa*, para que se investigaran las causas de las anomalías y se corrigieran las situaciones.

   Al 14 de marzo de 2016, no se mantenía un registro del seguimiento, el análisis y la solución de las anomalías e incidentes de seguridad detectados en los sistemas de información, ni la documentación relacionada para hacer referencia a las soluciones tomadas cuando estos se repitieran.

[4] Es un dispositivo digital lógico de interconexión de equipos, cuya función es interconectar dos o más segmentos de red.

[5] El grabador de vídeo digital (DVR, por sus siglas en inglés) es un dispositivo interactivo de grabación de televisión y vídeo en formato digital.

[6] Es un sistema o una red que está diseñada para bloquear el acceso no autorizado, y permitir al mismo tiempo comunicaciones autorizadas.

Criterio

Esta situación es contraria a lo que establece la *Política TIG-003* de la *Carta Circular 77-05*. En esta se dispone, entre otras cosas, que las agencias deberán desarrollar e 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. Además, deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos los límites para esos incidentes en términos de tiempo máximo y tiempo mínimo de respuesta. En consonancia con esto, para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados debieron mantener un registro, en el cual se anotaran los incidentes y cómo estos fueron resueltos, y preservar la documentación de los mismos.

Efectos

La situación comentada privó a la OSI de las herramientas y los mecanismos necesarios para identificar las debilidades existentes en la seguridad de los sistemas de información. Además, le impidió tener un control eficaz y documentado sobre el manejo de los incidentes ocurridos, con el objetivo de que se pudieran tomar las medidas para minimizar sus efectos y prevenir su reincidencia.

Causa

La situación comentada se atribuyó a que la directora de tecnología de información no impartió instrucciones al personal de la compañía contratada para que mantuviera un registro relacionado con la documentación del análisis de los incidentes que ocurrieron en los sistemas de información.

Véanse las recomendaciones 1 y 3.e.

RECOMENDACIONES

Al Secretario de Seguridad Pública

1. Ver que el comisionado del Negociado del Cuerpo de Emergencias Médicas de Puerto Rico cumpla con las **recomendaciones de la 2 a la 5** de este *Informe*. **[Hallazgos del 1 al 4]**

Al Comisionado del Negociado del Cuerpo de Emergencias Médicas de Puerto Rico

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

3. Ejercer una supervisión eficaz sobre el director de tecnología de información para que:

    a. Actualice y remita para su aprobación el *Plan* y se asegure de que incluya lo mencionado en el **Hallazgo 2-a.** Además, ver que se realicen pruebas y evaluaciones del mismo periódicamente para asegurar su efectividad y funcionamiento.

    b. Revise y actualice el *Plan de Respuesta de Emergencias y Recuperación*. Además, ver que se realicen pruebas y evaluaciones del mismo periódicamente para asegurar su efectividad y funcionamiento. **[Hallazgo 2-b.]**

    c. Configure los equipos que se utilizarán en el centro alterno identificado, y asegurarse de que el mismo no esté expuesto a los mismos riesgos que el lugar donde se encuentra el Negociado. **[Hallazgo 2-c.]**

d. Se asegure de que se redacten y remitan, para su aprobación, las normas y los procedimientos necesarios para administrar y controlar el acceso a las aplicaciones y los sistemas de información computadorizados. Las normas y los procedimientos deben incluir, entre otras cosas, el uso de un formulario o cualquier otra forma de documentación, que permita evidenciar la solicitud, autorización, modificación y cancelación de las cuentas de acceso a las aplicaciones y los sistemas de información. **[Hallazgo 3-a.]**

e. Imparta instrucciones al personal de la compañía contratada para que mantengan un registro relacionado con la documentación del análisis de los incidentes que ocurren en los sistemas de información. **[Hallazgo 4]**

4. Formalizar un acuerdo escrito que incluya los términos y las condiciones, bajo las cuales el Negociado utilizará los servicios de recuperación para la aplicación CAD, acordados verbalmente con el Negociado de Manejo de Emergencias y Administración de Desastres, en caso de emergencia. **[Hallazgo 2-d.]**

5. Ejercer una supervisión eficaz sobre la directora de Recursos Humanos y Relaciones Laborales, para asegurarse de que prepare y remita, para su aprobación, las políticas y los procedimientos de notificación a la OSI sobre la separación o el traslado del personal. **[Hallazgo 3-b.]**

APROBACIÓN

A los funcionarios y a los empleados del Negociado, 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

CUERPO DE EMERGENCIAS MÉDICAS DEL
ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dra. Rosana Otaño López	Directora Ejecutiva	24 ago. 15	24 jun. 16
Sra. Carmen Sánchez Colón	Directora de Tecnología de Información	24 ago. 15	24 jun. 16
Sr. José A. Vera Torres	Director de Recursos Humanos y Relaciones Laborales	24 ago. 15	24 jun. 16

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-08-32* del 27 de junio de 2008, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al 787-754-3030, extensiones 2801 o 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos y el tipo de opinión del informe.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el administrador de documentos al 787-754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr