INFORME DE AUDITORÍA TI-13-07

20 de septiembre de 2012

Corporación del Centro Cardiovascular de Puerto Rico y del Caribe

División de Informática y Telecomunicaciones

(Unidad 5217 - Auditoría 13492)

Estado Libre Asociado de Puerto Rico

Oficina del Contralor

San Juan, Puerto Rico

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **4**

OPINIÓN Y HALLAZGOS **4**

1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados 5

2 - Deficiencias relacionadas con la solicitud, la creación y el mantenimiento de las cuentas de acceso a los sistemas de información computadorizados 6

3 - Deficiencia en el registro de los respaldos de los archivos computadorizados de información 7

RECOMENDACIONES **9**

AGRADECIMIENTO **10**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **11**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **12**

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

20 de septiembre de 2012

Al Gobernador, al Presidente del Senado
y a la Presidenta de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la División de Informática y Telecomunicaciones (DIT) de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe (Centro Cardiovascular) para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procedimiento de las transacciones era adecuado. Efectuamos 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 6 de agosto de 2010 al 31 de marzo de 2011. 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, examen y análisis de informes y de documentos generados por la unidad auditada, pruebas y análisis de procedimientos de control interno y de otros procesos, y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene tres hallazgos sobre el resultado del examen de los controles internos establecidos para la administración del programa de seguridad, el acceso lógico a los sistemas de información computadorizados y la continuidad del servicio del Centro Cardiovascular.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Centro Cardiovascular se creó mediante la *Ley Núm. 51 del 30 de junio de 1986 (Ley Núm. 51)*, con el propósito de proveer tratamiento para enfermedades cardiovasculares a pacientes de Puerto Rico y del Caribe. Este funciona como una entidad independiente y separado de cualquier otra dependencia o instrumentalidad del Gobierno del Estado Libre Asociado de Puerto Rico. Está dirigido por una Junta de Directores (Junta) compuesta por siete miembros. Las funciones ejecutivas las realiza un Director Ejecutivo, nombrado por la Junta.

El Centro Cardiovascular es el organismo responsable de formular o ejecutar la política pública en relación con la planificación, la organización y la administración de los servicios cardiovasculares a rendirse en Puerto Rico. También efectúa, por medio de la Junta, la coordinación necesaria para sus fines y propósitos con el Departamento de Salud, el Recinto de Ciencias Médicas de la Universidad de Puerto Rico, la Administración de Servicios Médicos de Puerto Rico y los grupos privados envueltos en la prestación de servicios cardiovasculares en Puerto Rico.

Para llevar a cabo sus funciones el Centro Cardiovascular cuenta con la siguiente estructura organizacional: Junta de Directores, Dirección Ejecutiva, Oficina de Asesoramiento Legal, Área Operacional y el Área Clínica. El Área Operacional cuenta con los departamentos de Planificación y Análisis Financiero, Relaciones Públicas, Programas Institucionales, Gerencia de Materiales, Ingeniería, Servicios Generales, División de Informática y Telecomunicaciones, y Enfermería. El Área Clínica cuenta con los departamentos de Cirugía, Radiología, Servicios Médicos, Laboratorio, y Anestesia.

La DIT está dirigida por el Director Asociado y no tenía un presupuesto asignado. Los gastos de operación se sufragaban del presupuesto del Centro Cardiovascular, que para el año fiscal 2009-2010 fue $85,924,000.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta de Directores y de los funcionarios principales del Centro Cardiovascular, respectivamente, que actuaron durante el período auditado.

También cuenta con una página en Internet a la cual se puede acceder mediante la siguiente dirección: http://www.cardiovascular.gobierno.pr. 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* fueron remitidas al Director Ejecutivo, Lcdo. Javier E. Malavé Rosario, por carta de nuestros auditores del 26 de abril de 2011.

El 24 de mayo de 2011, el Director Ejecutivo remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados en la redacción del borrador de este *Informe*. Para algunos de estos **hallazgos**, luego de evaluar dichos comentarios y la evidencia remitida, determinamos que el Centro Cardiovascular tomó las medidas correctivas pertinentes.

El borrador de los **hallazgos** de este *Informe* se remitió al Director Ejecutivo para comentarios, por carta del 2 de agosto de 2012.

Mediante carta del 3 de agosto de 2012, el Director Ejecutivo indicó que no tenía observaciones sobre el borrador de los **hallazgos** de este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la DIT en lo que concierne a los controles internos para la administración del programa de seguridad, el acceso lógico a los sistemas de información computadorizados y la continuidad del servicio del Centro Cardiovascular se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 3** que se comentan a continuación.

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

Situación

a. Un análisis de riesgos de los sistemas de información computadorizados es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y que respondan a las posibles amenazas identificadas. El análisis de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 8 de agosto de 2011, en el Centro Cardiovascular no se había preparado por escrito un informe de análisis de riesgos de los sistemas de información computadorizados que cumpliera con los objetivos mencionados.

Criterios

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipo 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.

Efecto

La situación comentada impide al Centro Cardiovascular estimar el impacto que los elementos de riesgo tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Causa

La situación comentada se atribuye a que el Director Ejecutivo no había promulgado una directriz para la preparación y la documentación del análisis de riesgos de los sistemas de información del Centro Cardiovascular, según lo establecido en la *Carta Circular Núm. 77-05*.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Deficiencias relacionadas con la solicitud, la creación y el mantenimiento de las cuentas de acceso a los sistemas de información computadorizados

Situaciones

a. Al 23 de marzo de 2011, el Centro Cardiovascular tenía en operación una computadora en la que se procesaba una aplicación que consistía de los siguientes módulos: Nómina y Recursos Humanos, Farmacia, Cuentas por Pagar, Mayor General, Manejo de Materiales, Información del Paciente, Entrada de Órdenes, Récord Médico y Mantenimiento. La computadora contenía 721 cuentas de acceso activas. El examen efectuado a dichas cuentas reveló las siguientes deficiencias:

   1) Treinta y un usuarios tenían asignadas dos cuentas de acceso[1].

   2) No se habían eliminado las cuentas de acceso[1] de 12 empleados que cesaron sus funciones entre el 2 de agosto y el 29 de noviembre de 2010. Al 23 de marzo de 2011, habían transcurrido entre 114 y 233 días, desde la fecha de separación de estos exempleados.

[1] Los nombres de las cuentas de acceso se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Director Ejecutivo para comentarios.

Criterios

Las situaciones comentadas se apartan de lo establecido en la Sección b) del Título, *Contraseñas y Accesos al Sistema* de la *Norma Institucional Relacionada al Uso Apropiado de las Estaciones de Trabajo*; en la *Norma FMIS-025, Norma Institucional para la Remoción de Claves de Acceso del Centro Cardiovascular de Puerto Rico y el Caribe*; y en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05.*

Efectos

Las situaciones comentadas pueden propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, pueden propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en la aplicación sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

La situación comentada en el **apartado a.1)** se atribuye, principalmente, a que el Director Asociado de la DIT no ejerció la supervisión necesaria para asegurarse de que se eliminaran las cuentas duplicadas en el sistema.

La situación comentada en el **apartado a.2)** se atribuye, en parte, a que el Director de Recursos Humanos no informaba al Director Asociado de la DIT sobre el personal que cesaba sus funciones en el Centro Cardiovascular.

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

Hallazgo 3 - Deficiencia en el registro de los respaldos de los archivos computadorizados de información

Situación

a. La computadora principal del Centro Cardiovascular estaba configurada para que los datos, los programas y los procedimientos mantenidos en las librerías *FCSOLIB* y *FCSOLIBD* fueran respaldados en su totalidad en cintas magnéticas. El Operador de la Unidad Central del DIT era responsable de anotar el número de la cinta, el tipo de datos que contiene la misma, la fecha, la localización

y quién realizó el respaldo en el *Registro de Resguardo del Departamento de Informática y Telecomunicaciones*. El Centro Cardiovascular tenía alquilada una caja de seguridad en una compañía privada con el propósito de mantener dichos respaldos en un lugar seguro fuera de los predios donde está ubicado.

La inspección realizada el 8 de febrero de 2011, a las cintas almacenadas en la compañía privada y a la información del *Registro*, reveló que la información de 21 cintas de respaldo[2] (70 por ciento) de las 30 que estaban almacenadas en la compañía a dicha fecha no fue anotada en el *Registro*.

Criterio

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En consonancia con dicha política pública es necesario, entre otras cosas, mantener un inventario detallado de las cintas de respaldos para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para los respaldos y que permita, además, documentar el cumplimiento de las normas y los procedimientos establecidos.

Efectos

La situación comentada priva al Centro Cardiovascular de mantener un control adecuado de los respaldos almacenados en la compañía y dificulta la localización e identificación del contenido de los mismos. Esto, a su vez, podría afectar el proceso de restauración de los sistemas afectados en casos de emergencias.

Causa

La situación comentada se atribuye, principalmente, a que el Director Asociado de la DIT no ejerció la supervisión necesaria para asegurarse de que el *Registro* se mantuviera completo y actualizado.

Véanse las recomendaciones 1 y 3.b.

---

[2] La identificación de las cintas de respaldo se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Director Ejecutivo para comentarios.

RECOMENDACIONES

Al Secretario de Salud y Presidente de la Junta de Directores de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe

1. Ver que el Director Ejecutivo del Centro Cardiovascular cumpla con las **recomendaciones de la 2 a la 4. [Hallazgos del 1 al 3]**

Al Director Ejecutivo de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe

2. Asegurarse de que se realice y se documente el análisis de riesgos de los sistemas de información computadorizados, según se establece en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. El informe, producto de este análisis de riesgos, debe ser remitido para revisión y aprobación. **[Hallazgo 1]**

3. Ejercer una supervisión efectiva sobre el Director Asociado de la DIT para que se asegure de que:

   a. El empleado que tiene asignada las funciones de Administrador de la Red realice las gestiones necesarias para que:

      1) Efectúe las modificaciones necesarias a los sistemas, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 2-a.1)**.

      2) Elimine prontamente las cuentas de acceso de los empleados que hayan cesado sus funciones en el Centro Cardiovascular y vea que, en lo sucesivo, las cuentas se eliminen en el momento en que el empleado cesa. Esto, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 2-a.2)**.

   b. Registre la información de los respaldos que se encuentran fuera de los predios del Centro Cardiovascular requerida en el *Registro de Resguardo del Departamento de Informática y Telecomunicaciones*. **[Hallazgo 3]**

4. Ver que el Director de Recursos Humanos, en coordinación con el Director Asociado de la DIT, establezca un procedimiento para que se notifique a tiempo a la DIT el cese de un usuario en sus funciones, para la cancelación de la cuenta de acceso de este. **[Hallazgo 2-a.2)]**

AGRADECIMIENTO

A los funcionarios y a los empleados del Centro Cardiovascular, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor

Por: Yamín M Valdivieso

ANEJO 1

CORPORACIÓN DEL CENTRO CARDIOVASCULAR DE PUERTO RICO Y DEL CARIBE
DIVISIÓN DE INFORMÁTICA Y TELECOMUNICACIONES
MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Lorenzo González Feliciano	Secretario de Salud y Presidente de la Junta	6 ag. 10	31 mar. 11
Dr. Rafael Rodríguez Mercado	Rector Interino del Recinto de Ciencias Médicas de la Universidad de Puerto Rico y Vicepresidente de la Junta	6 ag. 10	31 mar. 11

ANEJO 2

CORPORACIÓN DEL CENTRO CARDIOVASCULAR DE PUERTO RICO Y DEL CARIBE
DIVISIÓN DE INFORMÁTICA Y TELECOMUNICACIONES

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lcdo. Javier E. Malavé Rosario, MHSA, CHE	Director Ejecutivo	6 ag. 10	31 mar. 11
Lcdo. Wilfredo Rabelo Millán, MHSA	Subdirector Ejecutivo	6 ag. 10	31 mar. 11
Sr. Arthur Fernández del Valle	Director de Planificación Financiera	6 ag. 10	31 mar. 11
Sr. Héctor Troche García	Director de Recursos Humanos	6 ag. 10	31 mar. 11
Sr. Eugenio Torres Ayala	Director Asociado de la DIT	6 ag. 10	31 mar. 11