Pedro L. González Uribe (Secretaría)

From: Y V G <yvg@ocpr.gov.pr>
Sent: Monday, June 27, 2022 6:18 AM
To: ppierluisi@fortaleza.pr.gov; gobernador@fortaleza.pr.gov; José Luis Dalmau Santiago (Presidente); Diana I. Dalmau Santiago (Sen. Dalmau Santiago); tatito@tatitohernandez.com; rahernandez@camara.pr.gov
Cc: gcastiel@fortaleza.pr.gov; Wanda Rivera (Sen. Dalmau Santiago); Secretaria; cortiz@camara.pr.gov; sopacheco@oslpr.org; biblioteca@oslpr.org; asepulveda@oslpr.org; Sub-ContralorTeam; Ejecutivos Div.TI; Giselle M. Agosto Clemente (Div.O); Nanceliz Serrano Cruz (Div.TI)
Subject: Informe de Auditoría TI-22-13 - Centro Cardiovascular de PR (Gobernador y presidentes Legislatura)
Attachments: TI-22-13.pdf

Estimado señor Gobernador y señores presidentes del Senado de Puerto Rico y de la Cámara de Representantes:

Les incluimos copia del *Informe de Auditoría TI-22-13* del área de Sistemas de Informática de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe, aprobado por esta Oficina el 17 de junio de 2022. Publicaremos dicho *Informe* en nuestra página en Internet: www.ocpr.gov.pr, para conocimiento de los medios de comunicación y de otras partes interesadas.

Agradeceremos que nos confirme el recibo de este correo electrónico a iplumey@ocpr.gov.pr.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,

Yesmín M. Valdivieso
Contralora

Anejo

INFORME DE AUDITORÍA TI-22-13

17 de junio de 2022

Corporación del Centro Cardiovascular de Puerto Rico y del Caribe

Sistemas de Informática

(Unidad 5217 - Auditoría 15524)

Período auditado: 26 de febrero al 30 de septiembre de 2021

CONTENIDO

Página

OBJETIVOS DE AUDITORÍA **2**

CONTENIDO DEL INFORME **3**

ALCANCE Y METODOLOGÍA **3**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **4**

COMUNICACIÓN CON LA GERENCIA **6**

CONTROL INTERNO **7**

OPINIÓN Y HALLAZGOS **7**

1 - Análisis de riesgos que no incluía un inventario de los activos de sistemas de información computadorizados del Centro Cardiovascular, y su clasificación 8

2 - Deficiencias relacionadas con el plan de contingencia y falta de un centro alterno para la recuperación de las operaciones computadorizadas 9

3 - Deficiencias relacionadas con el almacenamiento y el control de los respaldos del sistema Optimum 12

4 - Deficiencias relacionadas con los parámetros de seguridad configurados en el servidor principal; y falta de revisiones periódicas de las bitácoras de actividad de su sistema operativo 14

5 - Falta de inactivación de cuentas de acceso; y deficiencias relacionadas con la justificación y la aprobación de los privilegios de acceso remoto 18

RECOMENDACIONES **21**

APROBACIÓN **23**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **24**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **25**

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

17 de junio de 2022

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 del área de Sistemas de Informática de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe (Centro Cardiovascular). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones del área de Sistemas de Informática del Centro Cardiovascular se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

Evaluar el cumplimiento del *Manual Administrativo - Políticas Institucionales* (*Manual Administrativo*), aprobado el 20 de mayo de 2021 por la Junta de Directores (Junta), y de las políticas incluidas en 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 entonces director de la Oficina de Gerencia y Presupuesto, entre otros, para determinar lo siguiente:

1. El *Risk Analysis* incluye los elementos principales de un análisis de riesgos y está actualizado.

2. Los respaldos del sistema Optimum y de los registros de eventos de seguridad del servidor principal se preparan regularmente, y se mantienen en un lugar seguro fuera de los predios del Centro Cardiovascular.

3. El *Plan de Contingencia* incluye los elementos principales y está actualizado; y el Centro Cardiovascular cuenta con un centro alterno para la recuperación de las operaciones computadorizadas.

4. Las políticas de cuentas y locales fueron configuradas en el servidor principal; y los registros de eventos de seguridad se producen y están disponibles para su verificación.

5. Las versiones del sistema operativo y del antivirus, instalados en el servidor principal, se mantienen actualizadas.

6. La separación de los exempleados y excontratistas se informa al área de Sistemas de Informática y las cuentas de acceso de estos se inactivan.

7. Las autorizaciones de las cuentas con privilegios de acceso remoto a la red se documentan y justifican.

CONTENIDO DEL INFORME

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 26 de febrero al 30 de septiembre de 2021. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de auditoría. En

consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como, entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada; y pruebas y análisis de procedimientos de control interno y de otros procesos.

Para realizar esta auditoría, utilizamos el *Manual de Operaciones*[1], aprobado en agosto de 2009 por el entonces director ejecutivo; y las políticas establecidas en el *Manual Administrativo* y en la *Carta Circular 140-16*.

Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica las guías establecidas en el *Federal Information System Controls Audit Manual* (*FISCAM*)[2], emitido por el GAO. Aunque al Centro Cardiovascular no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Centro Cardiovascular se creó mediante la *Ley Núm. 51 del 30 de junio de 1986* con el propósito de proveer tratamiento para enfermedades cardiovasculares a pacientes de Puerto Rico y del Caribe. Este funciona como una entidad independiente y separada de cualquier otra dependencia o entidad del Gobierno de Puerto Rico. Está dirigido por una Junta compuesta por 7 miembros, de los cuales 4 miembros[3] son nombrados por el gobernador de Puerto Rico y 3 miembros[4] son *ex officio*. El presidente de

[1] El *Manual de Operaciones* se encuentra vigente y en proceso de revisión.

[2] El *FISCAM* utiliza las guías emitidas por el National Institute of Standards and Technology.

[3] Un representante de la Sociedad Puertorriqueña de Cardiología, 1 representante de una fundación de cardiología sin fines pecuniarios; y 2 representantes de la comunidad.

[4] El secretario de Salud, el rector del Recinto de Ciencias Médicas de la Universidad de Puerto Rico y el director ejecutivo de la Administración de Servicios Médicos de Puerto Rico.

la Junta es el secretario de Salud y las funciones ejecutivas las realiza un director ejecutivo nombrado por la Junta. Además, el Centro Cardiovascular cuenta con un director médico, nombrado por la Junta. Este le responde al director ejecutivo, excepto en los asuntos médicos, que le responde a la Junta.

El Centro Cardiovascular es el organismo responsable de formular o ejecutar la política pública en relación con la planificación, organización, operación y 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 sectores privados involucrados en la prestación de servicios cardiovasculares en Puerto Rico.

Para llevar a cabo sus funciones, el Centro Cardiovascular cuenta con la Junta de Directores; Asesoría Legal; Cumplimiento Corporativo; Facultad Médica; Dirección Ejecutiva; y Dirección Médica. Bajo la Dirección Ejecutiva se encuentran un director y un subdirector ejecutivo que supervisan al administrador asociado del ejecutivo; y las áreas operacionales y clínicas del Centro Cardiovascular. El área operacional se compone de Ingeniería; Planificación y Análisis Financiero; Programas Institucionales; Recursos Humanos; Relaciones Públicas; Servicios Generales; y Sistemas de Informática. El área clínica se compone de Anestesia; Centro de Imágenes; Cirugía; Enfermería; Laboratorio Clínico/Patología; Medicina; Sala de Emergencia; y Utilización y Revisión Médica.

El área de Sistemas de Informática le responde al director ejecutivo y es dirigida por 1 director asociado en informática. Cuenta con 1 supervisor de informática; 1 especialista en telecomunicaciones; 1 operador unidad central de informática; y 1 asistente gerencial principal. Al 31 de enero de 2021, el área tenía 3 puestos vacantes: 1 director de informática, 1 operador unidad central informática y 1 técnico de telecomunicaciones.

Al 3 de mayo de 2021, el área de Sistemas de Informática contaba con un centro de cómputos en el que se mantenía en operación una red de área local (LAN, por sus siglas en inglés) constituida por 29 servidores, 21 virtuales y 8 físicos, para el manejo de sus operaciones.

Los gastos de operación del área de Sistemas de Informática son sufragados del presupuesto del Centro Cardiovascular que, para los años fiscales del 2019-20 al 2021-22, ascendieron a $72,231,000, $76,021,000 y $78,338,000, respectivamente.

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

El Centro Cardiovascular cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.agencias.pr.gov/agencias/Cardio. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Mediante correo electrónico del 1 de abril de 2022, remitimos el borrador de este *Informe* para comentarios del Lcdo. Javier A. Marrero Marrero, director ejecutivo del Centro Cardiovascular.

El 13 de abril de 2022 el director ejecutivo contestó e indicó lo siguiente:

> Estamos en acuerdo con los hallazgos y contenido que expone el informe de borrador presentado por la Oficina del Contralor de Puerto Rico, sin embargo, los documentos en respuesta emitidos por nosotros establecen los proceso para mitigar y atender cada uno de los hallazgos presentados con la debida acción correctiva. [*sic*]

Luego de evaluar los comentarios y la evidencia suministrada, determinamos que el director ejecutivo tomó las medidas pertinentes para corregir varias situaciones, por lo que determinamos eliminarlas. Las restantes situaciones prevalecieron y se incluyen en este *Informe*.

CONTROL INTERNO

La gerencia del Centro Cardiovascular es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de lo siguiente:

- 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 Centro Cardiovascular.

En los **hallazgos** se comentan las deficiencias de controles internos significativos, dentro del contexto de los objetivos de nuestra auditoría, identificada 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 del área de Sistemas de Informática y del Centro Cardiovascular objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que los controles establecidos eran efectivos. Esto excepto por los **hallazgos del 1 al 5**, que se comentan a continuación.

Hallazgo 1 - Análisis de riesgos que no incluía un inventario de los activos de sistemas de información computadorizados del Centro Cardiovascular, y su clasificación

Situación

a. Un análisis de riesgos es un proceso mediante el cual se identifican los activos de los sistemas de información, sus vulnerabilidades y las amenazas a las que están expuestos. Además, se establecen medidas de seguridad y controles adecuados para evitar o disminuir los riesgos y proteger los activos.

Las entidades gubernamentales deben 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 o maliciosa. Para esto, deben realizar un análisis de riesgos que incluya un inventario de los activos de sistemas de información actualizados, que considere el equipo, los programas y los datos. Todos los activos deben ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deben ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer lo que se va a proteger.

El 30 de agosto de 2017 se otorgó un contrato a una compañía por $14,950 para realizar un análisis de vulnerabilidad de riesgos en los sistemas de información. El 15 de abril de 2021 el director asociado en informática nos suministró el *Risk Analysis* del 22 de diciembre de 2017, preparado por la compañía.

El examen realizado el 12 de mayo de 2021 reveló que el *Risk Analysis* no incluía un inventario de activos de sistemas de información, que considerara el equipo, los programas y los datos del Centro Cardiovascular. Tampoco incluía la clasificación de estos activos de acuerdo con el nivel de importancia para la continuidad de las operaciones, ni recomendaciones para implementar controles para proteger los mismos.

Criterio

La situación comentada es contraria a lo establecido en la Sección A. de la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*.

Efecto

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

Causa

El director asociado en informática atribuyó la situación a que, al momento de la preparación del análisis de riesgos, el entonces director asociado de Sistemas de Informática, encargado de solicitar los servicios de la compañía que preparó el *Risk Analysis*, no consideró que, como parte de este, se incluyera un inventario de los activos de sistemas de información.

Véanse las recomendaciones 1 y 2.a.

Hallazgo 2 - Deficiencias relacionadas con el plan de contingencia y falta de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Toda entidad gubernamental debe contar con un plan de contingencias para restablecer sus operaciones más importantes en caso de que surja una emergencia. Dicho plan debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de sus sistemas de información computadorizados.

   Mediante correo electrónico del 6 de mayo de 2021, la coordinadora de ambiente de cuidado y manejo de riesgo solicitó los planes de contingencia a las diferentes áreas del Centro Cardiovascular. Dichos planes tienen que incluir cómo responden las áreas ante una activación por emergencias o desastres, de acuerdo con la naturaleza de los servicios que estas ofrecen.

Como resultado de dicha solicitud, al 7 de junio de 2021, el área de Sistemas de Informática contaba con el *Plan de Contingencia* (*Plan*), revisado al 26 de mayo de 2021, por el director asociado en informática.

El examen realizado al *Plan* reveló que este no incluía los siguientes requisitos que son necesarios para atender las situaciones de emergencia:

1) El nombre del encargado de activar el *Plan* y de los integrantes de los grupos de recuperación, las responsabilidades asignadas a cada uno de ellos y los procedimientos detallados de cómo se llevarán a cabo los procesos para continuar realizando las tareas de su área.

2) Las condiciones tecnológicas actuales del Centro Cardiovascular.

3) El plan general de acción identificado por grupos y tareas de forma secuencial.

4) Los datos actualizados, y los números de contrato y de teléfono de emergencia de los proveedores primarios.

5) Los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información.

6) Un inventario de equipos, sistemas operativos, aplicaciones y archivos críticos de los sistemas de información. Tampoco incluía el detalle sobre los equipos de telecomunicaciones y de computadoras compatibles con los del Centro Cardiovascular.

7) Un detalle de toda la configuración crítica y del contenido de los respaldos, y el nombre de las librerías y de los archivos.

8) Un itinerario de restauración que incluya el orden de las aplicaciones y los procedimientos para restaurar los respaldos.

b. 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 una entidad pública o privada de similar configuración y tamaño; una compañía dedicada a servicios de restauración o un centro alterno de la propia entidad.

Nuestro examen reveló que, al 19 de agosto de 2021, el Centro Cardiovascular no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

Criterio

Las situaciones comentadas son contrarias a lo establecido en el Capítulo 3.5, Contingency Planning, del *FISCAM*.

Efectos

La situación comentada en el **apartado a.** puede 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, y de interrupciones prolongadas en los servicios provistos a los usuarios y a los clientes del Centro Cardiovascular.

La situación comentada en el **apartado b.** podría afectar las operaciones del Centro Cardiovascular, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales del Centro Cardiovascular.

Causas

La situación comentada en el **apartado a.** se debió, en parte, a que el director asociado en informática identificó que el *Plan* no era efectivo; y prefirió entregar a la coordinadora de ambiente de cuidado y manejo de riesgo una revisión del *Plan* sin actualizar, hasta que reciba un plan que contenga los elementos necesarios.

El director asociado en informática atribuyó la situación comentada en el **apartado b.** a que en el Centro Cardiovascular no se había contemplado tener un lugar alterno para recuperar las operaciones críticas en casos de emergencia.

Véanse las recomendaciones 1, y 2.b. y c.

Hallazgo 3 - Deficiencias relacionadas con el almacenamiento y el control de los respaldos del sistema Optimum

Situaciones

a. El área de Sistemas de Informática contaba con el *Manual de Operaciones*, en el que se establece la preparación de un respaldo diario incremental, y de respaldos semanales, mensuales y anuales completos. Los respaldos anuales se deben preparar el 30 de junio de cada año. Además, establece que los respaldos diarios y semanales se deben mantener en la bóveda interna del área de Sistemas de Informática, y los mensuales y anuales se deben llevar a la bóveda externa. Las cintas de los respaldos semanales se deben reutilizar mensualmente y las de los respaldos mensuales, anualmente. Las cintas anuales no se reutilizarán. El operador unidad central de informática o el director asociado en informática deben anotar las cintas en el *Registro de Respaldos*, en el que se les debe asignar un número e indicar qué tipo de datos contiene, la fecha, lugar donde se encuentra la cinta y quién realizó el respaldo. También establece los días específicos en los que se deben llevar las cintas a la bóveda externa, y que el operador unidad central de informática debe imprimir una lista de las cintas enviadas y recogidas.

   El supervisor de informática y el operador de la unidad central de informática eran los responsables de realizar los respaldos del sistema Optimum, donde se maneja el expediente médico electrónico del paciente. Para el almacenamiento de las cintas de respaldo, el área de Sistemas de Informática contaba con una bóveda interna[5] localizada

[5] Armario adaptado como bóveda.

dentro del cuarto de servidores. Además, fuera de los predios del Centro Cardiovascular contaban con una caja de seguridad arrendada a una compañía externa.

El examen realizado el 20 de julio de 2021 de los respaldos del sistema Optimum, producidos entre el 1 de julio de 2018 y el 30 de junio de 2021, disponibles en la caja de seguridad arrendada y en la bóveda interna del área de Sistemas de Informática, reveló las siguientes deficiencias:

1) En la caja de seguridad arrendada no se localizaron las cintas de nueve respaldos mensuales del sistema Optimum, correspondientes al año terminado el 30 de junio de 2021. En la caja solo se mantenían almacenadas tres cintas, correspondientes a agosto de 2020; y a mayo y junio de 2021.

2) En la caja de seguridad arrendada no se localizaron los respaldos anuales del sistema Optimum, correspondientes al 30 de junio de 2019 y de 2020.

3) No se utilizaba el *Registro de Resguardos* para documentar la preparación de los respaldos.

Criterio

Las situaciones comentadas son contrarias a lo establecido en las secciones A. y F. del apartado VI., Resguardos, del *Manual de Operaciones*.

Efectos

Las situaciones comentadas pueden ocasionar la pérdida de la información del expediente médico electrónico del paciente sin la posibilidad de poder recuperarla, lo que afectaría adversamente la continuidad de las operaciones del Centro Cardiovascular.

Las situaciones comentadas en el **apartado a.1) y 2)** puede ocasionar que, en casos de emergencia, el Centro Cardiovascular no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

La situación comentada en el **apartado a.3)** dificulta la localización e identificación del contenido de las cintas de respaldos, lo que podría afectar el proceso de restauración de la información o que se reutilicen las cintas fuera del período de conservación de estas. Además, limitó el alcance de nuestro examen para determinar si los respaldos se prepararon de acuerdo con lo establecido en la reglamentación.

Causas

La situación comentada en el **apartado a.** se atribuye a que el operador de la unidad central de informática no siguió el procedimiento incluido en el *Manual de Operaciones*. Además, el supervisor de informática y el director asociado en informática no verificaron que se trasladaran las cintas de respaldos mensuales a la caja de seguridad en la bóveda externa. La situación comentada en el **apartado a.2)** también se debió a que el supervisor de informática consideró que, al ser completos (*full backup*), los respaldos mensuales preparados cumplían con el requisito de un respaldo anual.

Véanse las recomendaciones 1 y 2.d.

Hallazgo 4 - Deficiencias relacionadas con los parámetros de seguridad configurados en el servidor principal; y falta de revisiones periódicas de las bitácoras de actividad de su sistema operativo

Situaciones

a. Los controles de acceso limitan y detectan los accesos inapropiados a los recursos de tecnología (datos, equipos e instalaciones), y los protege de modificación no autorizada, pérdida y divulgación. Estos controles incluyen tanto los lógicos como los físicos. Los controles de acceso lógico requieren que los usuarios se autentiquen, mediante el uso de contraseñas u otros identificadores, y limitan los archivos y demás recursos a los que pueden acceder, y las acciones que pueden realizar.

Las entidades gubernamentales son responsables de diseñar y mantener la seguridad de sus sistemas de información, por lo que deben asegurarse de lo siguiente:

- Establecer formalmente políticas de cuentas (*password policy* y *account lockout policy*) basadas en riesgos, y requerir su cumplimiento.
- Limitar los intentos para acceder al sistema con una contraseña errónea, para asegurar que esta no pueda ser descifrada.
- Establecer, en las políticas y los procedimientos de la entidad, criterios para identificar los eventos significativos del sistema que se deben registrar.
- Establecer procesos que permitan examinar las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

Para llevar a cabo las operaciones y brindar sus servicios, el Centro Cardiovascular contaba con un servidor principal configurado como *primary domain controller*, mediante el cual se controlaba el acceso a los recursos de la red.

Los exámenes efectuados el 25 de mayo y el 24 de agosto de 2021 sobre los parámetros de seguridad configurados en el sistema operativo de dicho servidor, revelaron que las siguientes políticas no estaban definidas:

1) La política relacionada con las contraseñas de las cuentas de acceso (*password policy*) para requerir inactivar el almacenamiento de las contraseñas mediante un cifrado reversible para todos los usuarios en el Dominio, de manera que estas no puedan ser descifradas. (*store password using reversible encryption*)

2) Las políticas de control de cuentas (*account lockout policy*) para establecer lo siguiente:

a) El tiempo que debía permanecer la cuenta inactiva por intentos de acceso sin éxito. (*account lockout duration*)

b) Un término de, al menos, tres intentos de acceso sin éxito, para que el sistema inactive automáticamente las cuentas. (*account lockout threshold*)

c) El tiempo para reiniciar el conteo de intentos de acceso sin éxito. (*reset account lockout counter after*)

b. Las entidades deben contar con procesos que permitan revisar las actividades de los usuarios en aquellos activos sensitivos que así lo ameriten. En la *Política MIS-010*, *Examen de Bitácoras de Actividad del Sistema* (*activity logs*), del *Manual Administrativo*, se indica que el Centro Cardiovascular debe realizar revisiones periódicas de las bitácoras de actividad de los sistemas computadorizados para minimizar las violaciones a la seguridad de la información de salud protegida. Esto permite evaluar los riesgos y las vulnerabilidades de los sistemas que manejan la información de salud, y desarrollar, implementar, mantener y actualizar salvaguardas administrativos, físicos y técnicos de seguridad, de acuerdo con lo requerido por la legislación o reglamentación estatal o federal aplicables.

Nuestro examen reveló que, al 25 de mayo de 2021, el supervisor de informática, quien estaba encargado de administrar la red, no revisaba periódicamente las bitácoras de actividad de eventos de seguridad provistos por el sistema operativo del servidor principal. Esto es necesario 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.

Criterios

Lo comentado es contrario a lo establecido en la Sección E.11 de la *Política ATI-003* de la *Carta Circular 140-16*, y en el Capítulo 3.2, Access Controls, del *FISCAM*.

La situación comentada en el **apartado a.1)** es contraria a lo establecido en el procedimiento 10.b. de la *Política MIS-007, Manejo de Contraseñas*, del *Manual Administrativo*.

Lo comentado en el **apartado b.** es contrario a lo establecido en la *Política MIS-010* del *Manual Administrativo*.

Efectos

Las situaciones comentadas pueden propiciar que personas no autorizadas accedan a información confidencial mantenida en los sistemas computadorizados y puedan hacer uso indebido de esta. Además, puede propiciar 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.

Además, lo comentado en el **apartado b.** expone al Centro Cardiovascular a pleitos judiciales o sanciones innecesarios, ante violaciones de seguridad que comprometan la información de salud protegida.

Causas

Las situaciones comentadas en el **apartado a.** se atribuyen a que el supervisor de informática estableció la configuración de los parámetros de seguridad de acuerdo con su juicio y experiencia. Además, lo comentado en el **apartado a.1)** se atribuyen a que este no siguió los procedimientos establecidos en la *Política MIS-007*.

Lo comentado en el **apartado b.** se debía en parte a que el supervisor de informática no siguió el procedimiento establecido en la *Política MIS-010*, porque lo descrito en esta no le era práctico por el tiempo que toma realizar las revisiones y el poco personal con el que cuenta el área de Sistemas de Informática.

Véanse las recomendaciones 1, y 2.e. y f.

Hallazgo 5 - Falta de inactivación de cuentas de acceso; y deficiencias relacionadas con la justificación y la aprobación de los privilegios de acceso remoto

Situaciones

a. Las entidades gubernamentales deben implementar controles de acceso para la utilización de la información y los programas de aplicación, de forma que estos sean accedidos solo por el personal autorizado. Las cuentas de acceso a los sistemas de información deben administrarse para controlarlas eficazmente e identificar y autenticar a los usuarios. Además, se deben revisar periódicamente las listas de autorizaciones de las cuentas de accesos a los sistemas de información para determinar si son apropiadas. También la entidad debe asegurarse de que los administradores de las cuentas reciban una notificación cuando los usuarios de los sistemas de información cesan funciones o se transfieren para que se eliminen, inactiven o aseguren las cuentas de acceso asignadas.

   Para garantizar la seguridad de la información almacenada en sus sistemas de información y limitar el acceso a información privilegiada y protegida, el Centro Cardiovascular debe eliminar los accesos al sistema computadorizado, de los empleados y contratistas que ya no trabajan o no tengan relación contractual con estos. La *Política MIS-011, Remoción de Claves de Acceso*, del *Manual Administrativo,* establece que el área de Recursos Humanos le requiere al empleado, en su proceso de liquidación, que acuda al área de Sistemas de Informática para que sus accesos se remuevan. Para esto, el empleado debe acudir, luego de haber recogido las firmas en el formulario *Proceso de Liquidación a la Terminación de Empleo* (formulario de *Liquidación*), y solicitar que remuevan sus accesos a los sistemas de información.

   Además, establece que cada gerente o supervisor que tenga empleados por contrato en su área con acceso a los sistemas de información está obligado a comunicar inmediatamente al director del área de Sistemas de Informática, mediante correo electrónico o comunicación telefónica, cuando el contratista termine sus trabajos.

Del 1 de julio de 2018 al 30 de abril de 2021, en el Centro Cardiovascular cesaron en sus funciones 157 empleados y 27 miembros de la facultad médica.

El examen realizado el 3 de junio de 2021 sobre el estatus de las cuentas de acceso otorgadas a estos reveló que 5 cuentas, pertenecientes a 4 exempleados y a 1 exmiembro de la facultad médica permanecían activas. Estos cesaron en sus funciones entre el 8 de diciembre de 2020 y el 15 de abril de 2021, por lo que, a la fecha de nuestro examen, habían transcurrido entre 49 y 177 días desde su cese o terminación. Las cuentas asignadas a uno de los exempleados y al exmiembro de la facultad médica contaban con privilegios de acceso remoto.

Una situación similar fue comentada en el *Informe de Auditoría TI-13-07* del 20 de septiembre de 2012.

b. Los sistemas de información del Centro Cardiovascular tienen la capacidad de ofrecer acceso remoto a los usuarios. Esto permite que se maximice el recurso y se facilite la información sin necesidad de que el usuario se encuentre físicamente en las instalaciones o utilice directamente los equipos electrónicos que son propiedad del Centro Cardiovascular. Dicho acceso debe ser otorgado solamente a personal autorizado, con necesidad de trabajar de manera remota, y luego de evaluar el pleno cumplimiento de las políticas de privacidad y seguridad. La *Política MIS-013, Acceso Remoto a los Sistemas de Información Protegida Electrónicamente - Red Privada Virtual* (*VPN*) establece que toda persona que solicite acceso remoto, ya sea empleado, contratista o miembro de la facultad médica, deberá, entre otras cosas, completar y firmar la *Solicitud para Acceso Remoto Cuenta VPN*. El personal del área de Sistemas de Informática se debe asegurar de que todos los formularios hayan sido completados y ofrecer su visto bueno para que se proceda con la autorización del acceso remoto, según solicitado.

Al 20 de julio de 2021, el Centro Cardiovascular contaba con 131 cuentas de acceso con privilegios de acceso remoto.

El examen efectuado el 5 de agosto de 2021 sobre el proceso para documentar la autorización y justificación de los privilegios otorgados a 25 de estas cuentas reveló las siguientes deficiencias en el área de Sistemas de Informática:

1) No contaba con los documentos justificantes para otorgar el privilegio de acceso remoto a 13 de estas cuentas (52%).

2) No se aseguró de que en 3 formularios (25%), correspondientes a las restantes 12 cuentas, se estableciera la fecha de vencimiento de la vigencia del acceso remoto.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política MIS-011* **[Apartado a.]** y en la *Política MIS-013* **[Apartado b.]** del *Manual Administrativo*.

Efectos

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

Además, la situación comentada en el **apartado a.** ocasionó que 2 cuentas de acceso, asignadas a exempleados, fueran utilizadas entre 8 y 94 días luego de la fecha de terminación de estos, sin que se pudiera identificar quién las accedió. Esto imposibilita la adjudicación de responsabilidades en los casos donde ocurran irregularidades dentro de los sistemas de información computadorizados del Centro Cardiovascular. Esta situación se agrava, debido a que el Centro Cardiovascular no realizaba una revisión de las bitácoras de actividad de eventos de seguridad. **[Véase el Hallazgo 4-b.]**

Causas

La situación comentada en el **apartado a.** se atribuye a que el personal del área de Sistemas de Informática no se aseguró de cancelar las cuentas de acceso a pesar de que firmó el formulario de *Liquidación* de los exempleados. Además, se atribuye a la falta de notificación, por parte de Dirección Médica, de la terminación de los acuerdos del miembro de la facultad médica con el Centro Cardiovascular.

Lo comentado en el **apartado b.1)** se debe, en parte, a que se otorgaron privilegios de acceso remoto a empleados del Centro Cardiovascular, por necesidad del servicio, durante la pandemia por COVID-19, que no fueron documentados.

La situación comentada en el **apartado b.2)** se atribuye, en parte, a que el personal del área de Sistemas de Informática que otorgó los privilegios de acceso remoto, no le requirió al gerente o supervisor que autorizó el formulario de *Solicitud para Acceso Remoto Cuenta VPN*, que estableciera la fecha límite para cancelar el privilegio.

Véanse las recomendaciones 1, 2.g. y 3.

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 2 y 3**. **[Hallazgos del 1 al 5]**

Al director ejecutivo de la Corporación del Centro Cardiovascular de Puerto Rico y del Caribe

2. Asegurarse de que el director asociado en informática cumpla con lo siguiente:

    a. Revise el *Risk Analysis* del área de Sistemas de Informática para que se incluya un inventario de los activos de sistemas de información, que considere el equipo, los programas y los datos del Centro Cardiovascular; y su clasificación de riesgos de acuerdo con el nivel de importancia para la continuidad de las

operaciones. Una vez revisado, lo remita para su aprobación y vea que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Centro Cardiovascular. **[Hallazgo 1]**

b. Actualice el *Plan* y lo remita para su revisión y aprobación, conforme a los aspectos comentados en el **Hallazgo 2-a.**

c. Identifique un centro alterno que no esté expuesto a los mismos riesgos del área de Sistemas de Informática, y se asegure de que el mismo cuente con la infraestructura y los equipos necesarios para restaurar las operaciones críticas computadorizadas del Centro Cardiovascular en caso de emergencia. **[Hallazgo 2-b.]**

d. Imparta instrucciones al supervisor de informática para que se asegure de que el operador unidad central de informática cumpla con lo siguiente:

   1) Realice las gestiones necesarias para mantener copias de los respaldos en un lugar seguro y fuera de los predios del Centro Cardiovascular. **[Hallazgo 3-a.1) y 2)]**

   2) Anote la información de los respaldos en el *Registro de Resguardo*. **[Hallazgo 3-a.3)]**

e. Evalúe las opciones correspondientes y defina la política de contraseña mencionada en el **Hallazgo 4-a.1)** y las políticas de control de cuentas que considere necesarias, de acuerdo con los riesgos y las amenazas de los sistemas de información del Centro Cardiovascular. **[Hallazgo 4-a.]**

f. Realice revisiones periódicas de las bitácoras de actividad, documente las mismas y, de ser necesario, tome de inmediato las medidas preventivas y correctivas. **[Hallazgo 4-b.]**

g. Imparta instrucciones al personal del área de Sistemas de Informática para que cumpla con las directrices establecidas en las siguientes políticas:

1) La *Política MIS-011* relacionada con la cancelación de las cuentas de accesos asignadas a los exempleados, una vez reciban y firmen los formularios de *Liquidación* de los exempleados. **[Hallazgo 5-a.]**

2) La *Política MIS-013* relacionada con el uso del formulario *Solicitud para Acceso Remoto Cuenta VPN* para documentar las autorizaciones de acceso remoto a los sistemas de información computadorizados del Centro Cardiovascular. Además, que requieran a los gerentes o supervisores que completen en todas sus partes dichos formularios. **[Hallazgo 5-b.]**

3. Asegurarse de que el director médico, en coordinación con el director asociado en informática establezca un procedimiento para notificar al área de Sistemas de Informática la terminación de los acuerdos de un miembro de la facultad médica con el Centro Cardiovascular, para la inactivación de la cuenta de acceso de este. **[Hallazgo 5-a.]**

APROBACIÓN

A los funcionarios y a los empleados del Centro Cardiovascular, 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 DEL CENTRO CARDIOVASCULAR
DE PUERTO RICO Y DEL CARIBE
SISTEMAS DE INFORMÁTICA

MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Carlos M. Mellado López	Presidente	26 feb. 21	30 sep. 21
Dra. Wanda T. Maldonado Dávila	Vicepresidenta	8 may. 21	30 sep. 21
Dr. Segundo Rodríguez Quilichini	Vicepresidente	26 feb. 21	7 may. 21
Lcdo. Jorge Matta González	Secretario	26 feb. 21	30 sep. 21

ANEJO 2

CORPORACIÓN DEL CENTRO CARDIOVASCULAR
DE PUERTO RICO Y DEL CARIBE
SISTEMAS DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Javier A. Marrero Marrero	Director Ejecutivo	26 feb. 21	30 sep. 21
Vacante	Subdirector Ejecutivo	26 feb. 21	30 sep. 21
Dr. Juan C. Sotomonte Ariza	Director Médico	26 feb. 21	30 sep. 21
Sr. Warker Rivas Cuba	Director Asociado en Informática	26 feb. 21	30 sep. 21

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