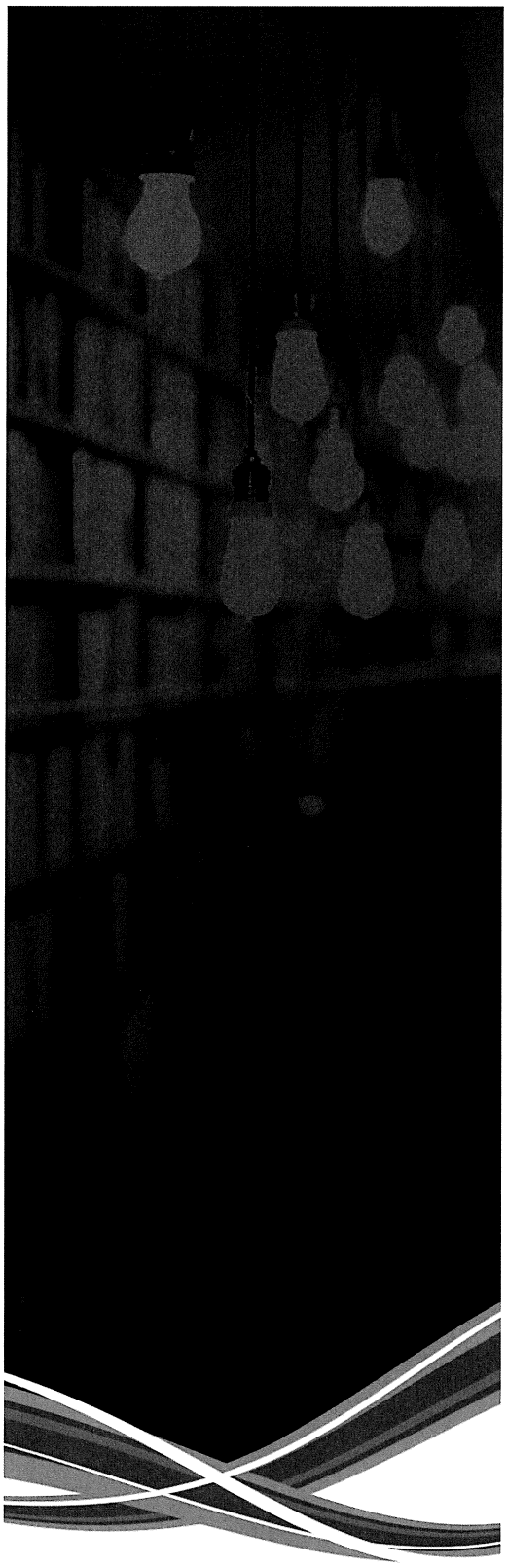

INFORME DE EXAMEN

OIG-E-21-008

EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN DEL CENTRO COMPRENSIVO DE CÁNCER DE LA UNIVERSIDAD DE PUERTO RICO

14 de mayo de 2021

OIG

OFICINA DE LA INSPECTORA GENERAL

GOBIERNO DE PUERTO RICO

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

La Oficina del Inspector General (OIG), en su rol de pre intervención realizó un examen, para conocer los protocolos y controles internos establecidos por la División de Sistemas de Información (DSI) del Centro Comprensivo de Cáncer de la Universidad de Puerto Rico (Centro Comprensivo). El objetivo del examen fue determinar si las operaciones del DSI se han implementado de acuerdo con las normas aplicables en todos los aspectos significativos, muy particularmente en lo que concierne a la efectividad de los controles internos para la administración de la seguridad, la continuidad del servicio, y el acceso físico y lógico.

Como resultado del examen realizado, se comentan las deficiencias de controles internos significativas dentro del contexto de los objetivos de nuestra pre-intervención, entre ellas: falta de un análisis de riesgos; planes para el manejo de incidentes; programas y planes para la continuidad de las operaciones en casos de emergencias; ausencia de un centro alterno; falta de un programa de concientización y adiestramiento al personal; ausencia de personal capacitado y adiestrado en seguridad y el manejo de *firewalls*[1]; deficiencias en la preparación de formularios de solicitud de acceso; y falta de independencia organizacional del DSI.

De igual forma, se añade un comentario especial en el presente informe ya que, como parte del análisis realizado se detectaron deficiencias en el manejo y control de la propiedad adscritas a la DSI que merecen ser atendidas y corregidas.

Este informe se hace público conforme con lo establecido en la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (Ley 15-2017); el Artículo 1.9 del Reglamento Núm. 9135, titulado como *Reglamento sobre Asuntos Programáticos de la Oficina del Inspector General;* y el Artículo 1.5 del Reglamento Núm. 9136, titulado como *Reglamento para la Publicación de Informes y Documentos Públicos Rutinarios de la Oficina del Inspector General de Puerto Rico*.

INFORMACIÓN SOBRE EL ÁREA EXAMINADA

El Centro Comprensivo fue creado por virtud de la Ley Núm. 230-2004, según enmendada, conocida como *Ley del Centro Comprensivo de Cáncer de la Universidad de Puerto Rico.* El propósito del Centro es ejecutar la política pública relacionada con la prevención, la orientación, la investigación y la prestación de servicios clínicos, y tratamientos relacionados con el cáncer en Puerto Rico. Para la consecución de los propósitos de la Ley el Centro estará afiliado mediante acuerdos con la Universidad de Puerto Rico.

---

[1] *Firewalls* - Según la empresa Cisco es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los poderes del Centro Comprensivo son ejercidos por una Junta de Directores (Junta) compuesta por 9 miembros. Estos son: el presidente de la UPR; el rector del Recinto de Ciencias Médicas; el secretario de Salud; el decano de la Escuela de Medicina; y otros 5 miembros nombrados por el gobernador con el consejo y consentimiento del Senado de Puerto Rico por un término de 4 años.

El presidente de la Junta es elegido por el gobernador y dicha Junta nombra al vicepresidente. Las funciones de administrar y dirigir el Centro Comprensivo las ejerce un director ejecutivo nombrado por la Junta. Además, cuenta con un subdirector ejecutivo que, a su vez, es el director médico del Hospital.

La estructura organizacional del Centro Comprensivo la componen las divisiones de: Medicina del Cáncer, la cual cuenta con el Hospital del Centro Comprensivo; del Control de Cáncer y Ciencias Poblacionales; de Biología del Cáncer; y de Apoyo a la Investigación y Educación; y la Oficina de Apoyo Administrativo. Esta última, es dirigida por el principal oficial financiero y operacional; las demás divisiones son dirigidas por un director que le responden al director ejecutivo.

La División de Sistemas de Información le respondía al administrador del Hospital que a su vez le respondía a la Junta de Gobierno y la División Medicina de Cáncer que le respondía al director ejecutivo del Centro. Al momento de nuestro examen el puesto de director de sistema de información estaba vacante. La división contaba con un gerente de sistema de información que realizaba las funciones del director, y le respondía al oficial asesor financiero, un administrador de sistemas y redes, un coordinador de la unidad de sistema, un especialista en sistema de información, un gerente de datos y un analista programador.

El Centro Comprensivo cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.cccupr.org. Esta página provee información acerca de los servicios que presta dicha entidad.

BASE LEGAL

El presente informe se emite en virtud de los Artículos 7, 8 y 9 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.

OBJETIVOS

El examen estuvo encaminado a determinar si las operaciones del DSI se han implementado de acuerdo con las normas aplicables en todos los aspectos significativos, particularmente en lo que concierne a la efectividad de los controles internos para la administración de la seguridad, la continuidad del servicio, y el acceso físico y lógico. A continuación, se enumeran algunas de las normas aplicables y utilizadas para evaluar cumplimiento:

- Ley Núm. 151-2004, según enmendada, conocida como *Ley de Gobierno Electrónico.*

- *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 Oficina de Gerencia y Presupuesto y las políticas que forman parte integral de la referida Carta Circular.
- *Las Prácticas Profesionales para la Gestión de Continuidad de Negocios* revisadas el 4 de abril de 2017.
- *Federal Information System Controls Audit Manual (FISCAM)* aprobado en febrero de 2009.
- El *Reglamento General del Centro Comprensivo de Cáncer de la Universidad de Puerto Rico* según enmendado el 2 de febrero de 2012, por la junta de directores del Centro Comprensivo.
- *CCCUPR Systems Security Policy*, aprobada el 13 de octubre de 2015, por el entonces director ejecutivo interino del Centro Comprensivo.
- *PRCCR Backup and Restore Procedure* aprobado el 22 de enero de 2013, por el entonces director interino del Registro del Centro Comprensivo de Cáncer de PR.
- *Computer Management Procedures,* fue efectivo el 27 de agosto de 2012 y aprobado el 8 de febrero de 2013, por el entonces subdirector ejecutivo del Centro Comprensivo.
- *Guía de Respaldo y Recuperación por Desastre* revisada el 20 de febrero de 2009.
- *Política Para el Control y Disposición de la Propiedad Mueble e Inmueble* aprobada por el director ejecutivo el 24 de septiembre de 2012.
- Entre otros.

ALCANCE Y METODOLOGÍA DEL EXAMEN

El examen cubrió el período del 1 de enero de 2020 al 30 de septiembre de 2020. Se efectuaron las pruebas que se consideraron necesarias a base de muestras y de acuerdo con las circunstancias.

La metodología utilizada fue la siguiente:

- Entrevistas a funcionarios y empleados.
- Inspecciones físicas.
- Exámenes y análisis de informes y de documentos generados por la unidad examinada o suministrado por fuentes externas.
- Pruebas y análisis de procedimientos de control interno y de otros procesos.
- Confirmaciones de información pertinente.

En algunos aspectos, se examinaron transacciones, documentos y operaciones de fechas anteriores y posteriores.

HALLAZGOS

A continuación, se detallan los hallazgos relacionados con las situaciones detectadas durante el transcurso del examen.

Hallazgo 1 – Falta de un informe de análisis de riesgos, de un análisis de impacto de negocio, de un plan para el manejo de incidentes del área de sistemas de información

Situación

a. El 2 de septiembre de 2020, se entrevistó al gerente de sistemas de información, quien nos informó que el Centro Comprensivo prepara un informe de análisis de riesgo, el cual se trabaja en el hospital, por lo que no es específico al área de sistemas de información. El 11 de septiembre, mediante entrevista, la administradora del hospital y directora de programas institucionales nos confirmó que el análisis de riesgo se realiza de forma general para las funciones del hospital.

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, clasificados de acuerdo con el nivel de importancia y de confidencialidad para la continuidad de las operaciones, sus vulnerabilidades y las amenazas a las que se encuentran expuestos (robos, desastres naturales, fallas, virus, acceso indebido a los datos, etc.), así como su 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.

b. Al 15 de septiembre de 2020, en el Centro Comprensivo no se había realizado un informe de análisis de impacto (*Business Impact Analysis o BIA* en inglés) para determinar los impactos cualitativos y cuantitativos cuando exista de una interrupción de los procesos críticos.

El análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por la pérdida o interrupción de las operaciones, y de las vulnerabilidades y amenazas que fueron identificadas y clasificadas en el análisis de riesgos. Además, debe proveer información para determinar las estrategias de recuperación más apropiadas.

Al 15 de septiembre de 2020, la División de Sistemas de Información (DSI) no tenía un procedimiento o plan para el manejo de incidentes en el que se estableciera, entre otras cosas,

una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos. Un plan de Manejo de Incidentes es una serie de actividades documentadas que serán ejecutadas por los diferentes grupos de continuidad de una agencia en respuesta a un incidente que interrumpa la prestación de sus servicios por un periodo determinado de tiempo.

c. Al 3 de agosto de 2020, el Plan Operacional de Emergencia del Centro Comprensivo no incluía las actividades, detalladas y específicas, de prevención y respuestas que llevaría a cabo el DSI ante cualquier desastre que cause interrupción en la prestación de los servicios del Centro Comprensivo. Un Programa de Manejo de Emergencias, tiene como propósito proteger y salvaguardar vidas y responder efectivamente ante la eventualidad de un desastre. Dicho programa debe incluir las actividades de prevención y de respuesta ante desastres naturales y de otros tipos en los que sea necesario activar los procedimientos de desalojo de las instalaciones.

d. Al 3 de agosto de 2020, el Centro Comprensivo no contaba con un Programa de Comunicación de Crisis que cumpliera con lo requerido en la *Política ATI-015, Programa de Continuidad Gubernamental.* No obstante, se nos proveyó un borrador titulado: Plan de manejo ante una situación de crisis, preparado por el relacionista público el 11 de agosto de 2020, 8 días después de nuestro requerimiento de información. El mencionado documento no establecía las guías reales, para enfrentar situaciones adversas y para asegurarse de que todo el personal y los portavoces estuviesen familiarizados con los procedimientos básicos de comunicaciones y su rol ante la eventualidad de crisis. Además, el documento carecía de la firma de las personas responsables de la preparación (Relacionista Público), revisión (Oficial del Programa de Seguridad y la Administradora y Directora de Programas Institucionales) y aprobación (Administradora y Directora de Programas Institucionales y Director Ejecutivo) del documento.

   Un Programa de Comunicación de Crisis tiene como propósito definir y proveer un canal formal y claro de comunicación existente en la entidad a nivel interno (empleados, junta de directores), externo (clientes, suplidores), autoridades y ante los medios de comunicación (Prensa, Radio, Televisión y otros) ante la eventualidad de un incidente y/o desastre.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política ATI-015, Programa de Continuidad Gubernamental,* de la *Carta Circular 140-16,* aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016, que establece lo siguiente:

Apartado C, Análisis de Riesgo y Análisis de Impacto Gubernamental, Numeral 1 establece que todas las agencias deben realizar un Análisis de Riesgos y un Análisis de Impacto dentro de un límite mínimo de tiempo de 24 meses y/o cuando se realice un cambio significativo dentro de su infraestructura operacional.

Apartado E, Plan de Manejo de Incidentes dispone que las agencias deberán desarrollar una estructura para el Manejo de Incidentes.

Apartado F, Programa de Manejo de Emergencias se establece que las agencias deberán desarrollar procedimientos de prevención, respuesta para cualquier tipo de desastre natural que cause interrupción en la prestación de sus servicios.

Apartado G, Programa de Comunicación de Crisis dispone que el referido programa deberá, entre otras cosas:

1. *Asignar los portavoces oficiales de la agencia.*
2. *Definir los medios de comunicación (Prensa, Radio, Televisión y otros).*
3. *Establecer las guías para enfrentar las situaciones adversas y para asegurarnos de que todo el personal y los portavoces están familiarizados con los procedimientos básicos de comunicaciones y su rol ante la eventualidad de una crisis.*
4. *Elaborar e implantar el Programa de Manejo de Comunicación de Crisis en base a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).*

Disposiciones similares a las indicadas en los apartados c, e, f y g de la ATI 015 se establecen en la *Política ATI-003, Seguridad de los Sistemas de Información,* aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016.

Efecto

Las situaciones comentadas en los **apartados (a)** y **(b)** impiden al Centro Comprensivo estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de ésta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificultan desarrollar un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Centro Comprensivo, en caso de que surja alguna eventualidad.

La situación comentada en el **apartado (c)** le impide al Centro Comprensivo tener un control eficaz y documentado sobre el manejo de incidentes. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas

con prontitud y aumentaría la extensión de los daños, si alguno. Por otro lado, la situación comentada en el **apartado (d)** puede propiciar la improvisación y, que, en casos de emergencias, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos onerosos de recursos y posibles interrupciones prolongadas de los servicios ofrecidos a los usuarios y a los clientes del Centro Comprensivo.

La situación comentada en el **apartado (e)** le impide al Centro Comprensivo contar con un canal formal y claro de comunicación interno y externo que establezca guías para enfrentar situaciones adversas y para asegurarse de que todo el personal y los portavoces estén familiarizados con los procedimientos básicos de comunicaciones y su rol ante la eventualidad de un incidente y/o desastre.

Causa

Las situaciones comentadas en los **apartados (a) y (b)** se atribuyen a que, no se había promulgado una directriz para la preparación del análisis de riesgos de los sistemas de información computadorizados y el análisis de impacto de negocios, como se establece en las *Políticas ATI-003* y *ATI-015.*

Las situaciones comentadas en los **apartados (c), (d) y (e)** se atribuyen, en parte, a que el puesto de director corporativo de los Sistemas de Información hacía dos años estaba vacante y no se habían impartido directrices al gerente de Sistemas de Información para el desarrollo y la aprobación del procedimiento para el manejo de incidentes. Además, se debió a que la administradora del Hospital entendía que, con el Plan Operacional de Emergencias y el Plan de Manejo ante una Situación de Crisis del Hospital, del Centro Comprensivo cumplía con lo requerido por las políticas, respecto estos programas.

Ver las recomendaciones 1, 2.a, 3, 4 y 6.a.1 al 3.

Hallazgo 2 – Ausencia de un plan de continuidad de negocios, de un plan de recuperación de desastres o contingencia sobre los sistemas de información, y de un centro alterno para la recuperación de las operaciones computadorizadas

Situación

a. Al 2 de septiembre de 2020, el Centro Comprensivo carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de los sistemas de información computadorizados. Esto era necesario para lograr el pronto funcionamiento de dichos sistemas y restaurar las operaciones en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. El Plan de Recuperación de Desastres (*Disaster Recovery Plan (DRP)* en inglés) establece las tareas, actividades y procedimientos formales que ejecuta la Unidad de Tecnología y Sistemas de Información conducentes al restablecimiento de los sistemas críticos de procesamiento de la agencia ante la eventualidad de un desastre o contingencia.

   Al 2 de septiembre de 2020, el Centro Comprensivo carecía de un DRP o contingencia que incluyera los siguientes requisitos para atender situaciones de emergencia:

   - Los procedimientos a seguir cuando el DSI no pueda recibir ni transmitir información de los usuarios que acceden mediante conexiones remotas a los sistemas de información.
   - La identificación de los archivos críticos del Centro Comprensivo.
   - Una lista detallada con todos los medios de comunicación de los diferentes miembros de cada grupo de recuperación.
   - El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones.
   - El detalle de toda la configuración de los equipos críticos (equipo de comunicación y servidores) y del contenido de los respaldos, así como los nombres de las librerías y los archivos.
   - El detalle de toda la configuración de los sistemas utilizados en el área de los sistemas de información y requeridos para efectuar una restauración en un centro de información alterno.
   - Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos.
   - Una lista de los proveedores principales que incluya el número de teléfono y el nombre del personal de enlace con la entidad.
   - Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

c. Al 2 de septiembre de 2020, el Centro Comprensivo no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alterno en las instalaciones de ésta.

Criterio

Las situaciones comentadas en los **apartados (a) y (b)** son contrarias a lo establecido en el Apartado B.1, Estructura de Continuidad de la *Política ATI-015, Programa de Continuidad Gubernamental,* de la *Carta Circular 140-16,* aprobada por el director ejecutivo de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016, la cual dispone que:

> *Es requerido que cada agencia establezca una estructura organizacional de continuidad. Los directores de las agencias serán los líderes del programa de*

continuidad de la agencia y serán responsables de la implantación y cumplimiento del programa en la agencia.

Por otro lado, en el *Apartado D, Plan de Recuperación de Desastres,* de la referida Política se establece que:

> *Todas las agencias deben tener implantado, ejercitado y probado su Plan de Recuperación de Desastres. El Plan de Recuperación de Desastres será actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.*

Además, la situación comentada en el **apartado (b)** es contraria a lo establecido en la *Guía de Respaldo y Recuperación de Desastre* del Centro Comprensivo la cual dispone en el *Artículo 7* que el equipo de recuperación ante desastre se reunirá anualmente para evaluar el documento y hacer recomendaciones para cambios a la guía.

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

Además, estas prácticas sugieren que, como parte integral del plan de continuidad de negocios, deben existir acuerdos con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos acuerdos debe incluirse también 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: **[Apartado c]**

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

Efecto

Las situaciones comentadas en los **apartados a y b** pueden propiciar la improvisación y, que, en casos de emergencias, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto

riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios ofrecidos a los usuarios y a los clientes del Centro Comprensivo.

La situación comentada en el **apartado c** podría afectar las operaciones del Centro Comprensivo, ya que no tendría 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 Comprensivo.

Causa

Las situaciones comentadas en los **apartados (a) y (b)** se atribuyen a la falta de un análisis de riesgos de los sistemas de información computadorizados del Centro Comprensivo que sirviera de base para la preparación y la revisión de un plan de continuidad de negocios que incluyera un plan de contingencia con los requisitos necesarios para atender eventos o situaciones de emergencia.

La situación comentada en el **apartado (c)** obedece a que no se habían realizado las gestiones necesarias para identificar un lugar disponible y adecuado como centro alterno para formalizar los acuerdos necesarios para la utilización de este en casos de emergencia.

Ver las recomendaciones 1, 2.b, 4, 6.a.4 al a.6 y 8.

Hallazgo 3 – Falta de un programa de concientización y adiestramiento, y de un programa de pruebas y ejercicios para la continuidad del Centro Comprensivo

Situación

a. Al 7 de agosto de 2020, el Centro Comprensivo no había implementado un programa de concientización y adiestramientos relacionado con la continuidad de los servicios sistemas de información computadorizados. El programa de concientización y de adiestramiento tiene como propósito promover en sus empleados el conocimiento de todas las actividades del Programa de Continuidad de la agencia. Además, permite que el personal esté habilitado para responder a los incidentes de una manera tranquila y eficiente.

b. Al 7 de agosto de 2020, el Centro Comprensivo no había implementado un programa de pruebas y ejercicios relacionado con la continuidad de los servicios de sistemas de información computadorizados ante la eventualidad de una interrupción de los procesos críticos del Centro Comprensivo. El programa de pruebas y ejercicios describe el diseño, desarrollo, ejecución, evaluación y validación de la funcionalidad de las actividades y procedimientos de mitigación, respuesta, recuperación, reanudación y de restauración para todas las funciones y procesos críticos de negocios de la agencia.

Criterio

Las situaciones comentadas en los **apartados (a)** y **(b)** son contrarias a lo establecido en los apartados H e I de la *Política ATI-015* de la Carta Circular 140-16, aprobada por el director ejecutivo de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016, que el Programa de Continuidad Gubernamental que las agencia establezcan deberán, entre otras cosas, elaborar e implementar:

> *Un Programa de Concientización y Adiestramientos a nivel básico, intermedio y avanzado basado en la responsabilidad de continuidad a ser realizada por los empleados.*
>
> *El programa de pruebas y ejercicios en base a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII) y documentar todos los ejercicios y pruebas de continuidad de los diferentes grupos de continuidad.*

Efecto

Las situaciones comentadas en los **apartados (a)** y **(b)** pueden propiciar la improvisación y, que, en casos de emergencias, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios ofrecidos a los usuarios y a los clientes del Centro Comprensivo.

Causa

Las situaciones comentadas en los **apartados (a)** y **(b)** se atribuyen, en parte, a que el puesto de director corporativo de los Sistemas de Información hacía dos años estaba vacante y no se habían impartido directrices para el desarrollo y la aprobación de los Programas mencionados. Además, obedece a que, los funcionarios que actuaron durante el periodo de emisión y vigencia de la *Carta Circular 140-16,* aprobada por el director ejecutivo de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016, no cumplieron con lo establecido en la misma y con las políticas o guías que forman parte integral de la referida *Carta Circular.* Por otro lado, al 17 de septiembre de 2020, la directora y el subdirector ejecutivo del Centro Comprensivo llevaban en sus puestos 5 y 2 meses, respectivamente, y desconocían lo establecido en la referida *Carta Circular* y las políticas que formaban parte integral de ésta.

Ver las recomendaciones 1, 2.c, 4 y 6.a.7.

Hallazgo 4 – Ausencia de personal capacitado y adiestrado en seguridad y en el manejo de *firewalls*

Situación

a. Al 9 de septiembre de 2020, el Centro Comprensivo no contaba con un personal capacitado ni adiestrado en la administración de la seguridad y firewalls de los sistemas computadorizados. El 7 de agosto de 2020, la directora asociada de Recursos Humanos nos certificó que el gerente de sistemas de información estaba a cargo de la seguridad de los sistemas de información del Hospital. No obstante, no constaba en sus expedientes evidencia de adiestramientos y certificaciones en el área de seguridad. Sin embargo, éste, mediante entrevista realizada el 2 de septiembre de 2020, indicó que la persona a cargo de la seguridad era el administrador de redes. Además, confirmó que ambos no contaban con las certificaciones requeridas en seguridad y en el manejo de firewalls.

La entidad utiliza *firewall* para las restricciones de tráfico y filtro de contenido. Sin embargo, ninguno de los empleados del DSI había tomado adiestramientos, cursos o certificaciones sobre el manejo de *firewalls*. El 9 de septiembre de 2020, la directora asociada de Recursos Humanos nos certificó que, en el plan de clasificación del Centro Comprensivo de Cáncer de la Universidad de Puerto Rico, no comprendía dentro de sus clases de puestos las clases de gerente de seguridad informática, especialista de seguridad informática y/o oficial de seguridad informática. No obstante, el hospital cuenta con un oficial de seguridad y ambiente de cuidado.

Criterio

La situación comentada es contraria a lo establecido en la *Políticas Núm. ATI-014, Manejo de Firewalls,* de la *Carta Circular 140-16,* aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016. Estas políticas sugieren que:

> *En agencias donde la complejidad de la seguridad lo requiera por necesidad de cumplimiento de regulaciones federales, tales como HIPPA, SOX, FISMA y otras leyes análogas, es recomendable que exista un Oficial de Seguridad Informática, Gerente de Seguridad Informática, Especialista en Seguridad Informática o sus equivalentes, debido a los retos técnicos que, regularmente, supone la implementación de políticas y controles para tal cumplimiento. Un candidato para las posiciones antes mencionadas debe tener una combinación entre educación, experiencia y adiestramiento para ser cualificado como experto en seguridad. En el caso del Oficial / Especialista en Seguridad Informática este debe cumplir al menos con los siguientes requisitos*:

- *Bachillerato en ingeniería (computadora, telecomunicaciones o campos relacionados), ciencias de computadoras o sistemas de información de una universidad acreditada.*
- *Poseer alguna de las siguientes certificaciones: CEH[2], OSCP[2], CHFI[3] o su equivalente.*
- *Cinco (5) o más años de experiencia en tareas relacionadas a la seguridad y cumplimiento de regulaciones federales.*

Por otro lado, el gerente de seguridad informática, además de, contar con la preparación académica antes mencionada, debe:

- *Poseer alguna de las siguientes certificaciones: CISSP[4] o su equivalente, GIAC[5] o su equivalente, CISM[6] o su equivalente.*
- *Diez (10) o más años de experiencia en el campo de las tecnologías de información con un historial sólido en seguridad de la información y en el área de cumplimiento de regulaciones federales y, al menos cinco (5) años en experiencia gerencial.*

Efecto

La ausencia de personal capacitado y adiestrado en seguridad y manejo de *firewalls* podría reducir la efectividad de los sistemas de información, exponer los activos y la información a riesgos innecesarios que afecten la continuidad de las operaciones del Centro Comprensivo.

Causa

Las situaciones comentadas se atribuyen a que los directores ejecutivos, el entonces principal oficial financiero y operacional y/o la administradora del hospital en funciones del Centro Comprensivo no les requirieron al director (a) y/o directora asociada de Recursos Humanos, a esa fecha, que creara dentro del Plan de Clasificación de Puesto del Centro Comprensivo la clase de oficial de seguridad informática, gerente de seguridad informática, especialista en seguridad informática o sus equivalentes, de manera que se reclutara el personal capacitado y adiestrado en seguridad y en el manejo de *firewalls*. Además, no se aseguraron de que tanto el gerente de sistemas como el administrador de sistemas y redes cumpliera con los adiestramientos y certificaciones necesarios para realizar las funciones que le fueron asignadas.

---

[2] *Certified Ethical Hacker* (CEH), *Offensive Security Certified Professional* (OSCP)[2], *Computer Hacker Forensic Investigator* (CHFI)[3], *Certified Information System Security Professional* (CISSP) [4], *Global Information Assurance Certification* (GIAC) [5], *Certified Security Information Manager* (CISM)[6]

Ver las recomendaciones 1, 4 y 7.a.

Hallazgo 5 – Falta de adiestramientos a los empleados de la División de Sistemas de Información y de un programa para divulgar al personal las normas y los procedimientos de seguridad de la información.

Situación

a. El 7 de agosto de 2020, la directora asociada de Recursos Humanos certificó que el Centro de Investigación y Desarrollo del Centro Comprensivo no contaba con un programa implementado para ofrecer dichos adiestramientos. Sin embargo, indicó que el Centro para el Control y Prevención de Enfermedades (CDC, por sus siglas en inglés) tenía una oferta de adiestramientos de los cuales los empleados que estuviesen interesados podían participar si así lo solicitaban. Ver LC-7.1-1 Certificación de Recursos Humanos.

   Los empleados del DSI no habían recibido adiestramientos relacionados con las tareas que se le habían sido asignadas, al menos en los últimos tres años. Estos adiestramientos son necesarios para asegurar que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con la seguridad de los sistemas de Información.

b. Al 7 de agosto de 2020, el Centro Comprensivo no contaba con un programa para divulgar al personal las normas y los procedimientos de seguridad de la información (*security awareness*). Mediante este se orienta a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la entidad y se da a conocer la reglamentación y la política pública relacionada con la seguridad de la misma. La directora asociada de Recursos Humanos nos certificó que el Centro de Investigación y Desarrollo del Centro Comprensivo, como parte de su protocolo de reclutamiento, hacía entrega del Manual del Empleado y que el Inciso 3.1 del mismo contenía las políticas de seguridad de los sistemas de información. No obstante, esto no debe sustituir un programa de concientización y adiestramiento sobre la importancia de mantener la seguridad de los sistemas de información.

Criterio

La situación comentada en el **apartado (a)** es contraria a lo establecido en el Apartado H de la *Política Núm. ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*, aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016, en la que se establece, entre otras cosas, que el personal de sistemas de información y telecomunicación deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.

La situación comentada en el **apartado (b)** es contraria a las mejores prácticas en el campo de la tecnología de información requieren que cada entidad gubernamental establezca e implemente un

programa para la divulgación de las normas y los procedimientos de seguridad de información a todos sus funcionarios y empleados. Un programa bien diseñado para la divulgación de las normas y los procedimientos de seguridad debe estar, primeramente, encaminado a crear conciencia de los riesgos a los cuales están expuestos los sistemas de información, y luego a desarrollar actitudes prácticas en los funcionarios y los empleados de una organización con el fin de promover la protección de los activos físicos y los de la información. La concienciación de los riesgos y las salvaguardas disponibles son las primeras líneas de defensa que se utilizan en la seguridad de los sistemas de información y de las redes de comunicación gubernamentales.

Efecto

La situación comentada en el **apartado (a)** podría reducir la efectividad de dichos sistemas y exponer la información a riesgos innecesarios que afecten la continuidad de las operaciones del Centro Comprensivo.

La situación comentada en el **apartado (b**) podría ocasionar el incumplimiento de las normas de seguridad con los consiguientes efectos adversos en cuanto a la protección de la información. Esto, a su vez, podría afectar la integridad, disponibilidad y confiabilidad de la información procesada por los usuarios.

Causa

Las situaciones comentadas se atribuyen a que el entonces principal oficial financiero y operacional y la administradora del hospital no les requirieron a la directora asociada de Recursos Humanos que implementara:

- Un programa para que los empleados del DSI recibieran los adiestramientos necesarios para realizar las funciones que le han sido asignadas **[Apartado a.]**

- Un programa para orientar a todos los empleados del Centro Comprensivo con relación a las normas y los procedimientos de seguridad de la información. **[Apartado b.]**

Ver las recomendaciones 1, 4, 7.b. y c.

Hallazgo 6 – Formularios de solicitud de acceso a la red incompletos

Situación

a. El examen de 10 formularios, *Solicitud de Acceso a Sistemas de Información del CCCUPR* preparados del 4 de marzo de 2020 al 16 de julio de 2020, encontramos que en 7 formularios (70 por ciento) faltaba parte de la información requerida, según se indica a continuación:

INFORMACIÓN REQUERIDA	CANTIDAD DE FORMULARIOS
Nombre del Supervisor	1
Visto Bueno del Supervisor y Fecha	5
Firma del Supervisor	1
# Licencia Profesional	1
Turno	8
# empleado del Supervisor	4
Firma del usuario	1

Criterio

La situación comentada es contraria a la *Política Núm. ATI-003, Seguridad de los Sistemas de Información, de* la *Carta Circular 140-16* aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016. En esta se establece, entre otras cosas, que 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.

Además, se establece que será política del Gobierno de Puerto Rico que cada agencia es responsable de diseñar y mantener la seguridad de sus sistemas de información. Esta norma se instrumenta, en parte, mediante los controles de acceso rigurosos a la red, programas y a los archivos, incluyendo el uso de formularios para solicitar la creación, modificación o eliminación de cuentas de acceso a los diferentes recursos disponibles a través de la red, para cada usuario conforme a sus necesidades. Dichos controles también requieren mantener registros completos, confiables y actualizados de las cuentas solicitadas y autorizadas.

Efecto

La situación comentada impide al Centro Comprensivo mantener un control adecuado sobre la administración de las cuentas y del equipo de computadoras. Además, propicia que personas no autorizadas puedan utilizar estas cuentas para lograr acceso a información confidencial mantenida en los sistemas de información y hacer uso indebido de esta. También, propicia 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. De igual forma,

impide al DSI mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios.

Causa

La situación comentada denota que los empleados concernidos del DSI no verificaban que dichos formularios fueran completados debidamente antes de crear las cuentas que eran solicitadas.

Ver las recomendaciones 1, 4, 6.a.8 y a.9.

Hallazgo 7 – Falta de revisión y aprobación de la reglamentación aplicable a los Sistemas de Información

Situación

La evaluación realizada el 5 de agosto de 2020, sobre la reglamentación aplicable a los sistemas de información del Centro Comprensivo reveló lo siguiente:

a. El Centro Comprensivo contaba con una política de seguridad, *CCCUPR Systems Security Policy,* aprobada el 13 de octubre de 2015, por el entonces director ejecutivo interino. El propósito de la política era asignar las responsabilidades para la seguridad lógica y física de la organización. Además, describir la seguridad necesaria para la integridad de la información, la protección de los activos frente a usuarios no autorizados, alteración y/o destrucción de la información y el procedimiento correcto para establecer un control adecuado para gestionar los incidentes de seguridad. En el examen realizado al referido documento se determinó que:

    1) La última revisión había sido realizada el 15 de julio de 2015, es decir, hacía 5 años no se revisaba. Sin embargo, en el documento se dispone que dicha política debe ser revisada, anualmente, por el director de sistemas de información del Centro Comprensivo comenzando desde la fecha de efectividad[3] de la misma. Ver páginas 1 y 13, del CCCUPR *System Security Policy*

    2) No se incluían disposiciones para establecer los mecanismos de capacitación relacionados con la seguridad y para mantener los conocimientos actualizados de los nuevos empleados, contratistas y usuarios. Tampoco, la forma cómo se divulgaría a los usuarios las normas y los procedimientos de seguridad de la entidad.

b. Las Normas de Uso de los Sistemas de Información configuradas como advertencias en la pantalla inicial de las computadoras que utilizan los usuarios indican que fueron resultado del

[3] La fecha de efectividad de la política según consta en el documento es el 25 de octubre de 2012.

Memorando OCP-98-391 de la Oficina del Contralor del 4 de mayo de 1998[4], por lo que no han sido revisada y atemperadas con la Política de Seguridad establecidas en el 2015.

c. El procedimiento para la administración de las computadoras, *Computer Management Procedures*, fue efectivo el 27 de agosto de 2012 y aprobado el 8 de febrero de 2013, por el entonces subdirector ejecutivo del Centro Comprensivo, es decir, hacía 7 años que no se revisaba. Ello, a pesar de, incluir una disposición que establece que el mismo debe ser revisado anualmente, a partir de la fecha de efectividad incluida en la política. Además, una de las dos personas que se mencionaban como los contactos para atender las situaciones que se presentan con el uso de las computadoras ya no trabajaba en el Centro Comprensivo.

d. La Guía de Respaldo y Recuperación por Desastre (La Guía) describe los métodos y procedimientos para ser utilizado por el Centro Comprensivo a fin de proteger y restaurar los datos y operaciones en el evento de un desastre. En el examen realizado al referido documento determinamos que:

   1) Hacía 11 años que no se revisaba.

   2) No estaba firmada por el director ejecutivo, principal oficial, el principal oficial financiero ni el director de sistemas de información.

   3) No estaba certificada de acuerdo a las prácticas profesionales de continuidad establecidas por el *Disaster Recovery Institute International* (DRII).

   4) Se recomendaba al *International Safe Deposit* como el lugar fuera de las instalaciones del centro para el almacenamiento de las copias de cintas de información, lo que es indicativo que a la fecha de preparación de la guía no tenían acuerdos con dicha compañía. Actualmente, el Centro Comprensivo tiene un contrato con la referida compañía.

   5) En el caso de incendio o desastre naturales de ser necesario mover el centro de sistemas de informática a una ubicación de seguridad o sitio activo, indicaba que la ubicación designada serían las facilidades clínicas que se desarrollarían, es decir, a esa fecha no estaban construidas. Como segunda opción, sugería la utilización de una compañía privada, cuando el Centro Comprensivo tuviera un sistema de virtualización. Por consiguiente, ninguna de las dos alternativas era viables a la fecha de redacción del documento.

   6) Las dos personas que componían el equipo de recuperación ya no trabajan para el Centro Comprensivo e incluso, a la fecha del informe, los puestos estaban vacante.

---

[4] Cabe señalar que la Oficina del Contralor derogó las Cartas Circulares OC-98-11 y la OC-06-13 titulada *Sugerencia sobre Normas y Controles para el uso de los sistemas computadorizados* del 30 de enero de 2005 y 28 de noviembre de 2005 respectivamente mediante la Carta Circular OC-15-19 del 30 de enero de 2015.

e. El Procedimiento de Resguardo y Restauración de la Información del Registro del Centro Comprensivo de Cáncer de PR, *PRCCR Backup and Restore Procedure*, fue revisado el 15 de diciembre de 2012 y aprobado el 22 de enero de 2013, por el entonces director interino, es decir, hacía7 años no se revisaba. En el referido Procedimiento se establece que la responsabilidad de mantener actualizado el mismo es la División de Sistemas de Información del Registro Central de Cáncer de Puerto Rico. No obstante, el 6 de agosto de 2020, 3 días después de un segundo requerimiento de información, el mencionado Procedimiento fue revisado, sin embargo, carecía de la firma del Administrador de Base de Datos de Sistemas de Información, del director interino del PRCCR y tampoco estaba aprobado por el director ejecutivo del Centro Comprensivo.

Criterio

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

Las mejores prácticas en el campo de la tecnología de información requieren que cada entidad gubernamental establezca e implemente un programa para la divulgación de las normas y los procedimientos de seguridad de información a todos sus funcionarios y empleados. Un programa bien diseñado para la divulgación de las normas y los procedimientos de seguridad debe estar, primeramente, encaminado a crear conciencia de los riesgos a los cuales están expuestos los sistemas de información, y luego a desarrollar actitudes prácticas en los funcionarios y los empleados de una organización con el fin de promover la protección de los activos físicos y los de la información. La concienciación de los riesgos y las salvaguardas disponibles son las primeras líneas de defensa que se utilizan en la seguridad de los sistemas de información y de las redes de comunicación gubernamentales. **[Apartado a.2]**

Las situaciones comentadas en los **apartados a.1, a.3, b** y **c.1, c.3 al c.6,** son contrarias a lo establecido en las respectivas políticas o procedimientos, las cuales requieren que las mismas sean revisadas anualmente.

Además, las situaciones comentadas en los **apartados c.2 y d** son contrarias a lo establecido en la Sección 3 del *Reglamento General del Centro Comprensivo de Cáncer de la Universidad de Puerto Rico* según enmendado el 2 de febrero de 2012, por la Junta de Directores del Centro Comprensivo en el cual se dispone que:

> *Todos los reglamentos o políticas operacionales del Centro serán aprobados por el Director Ejecutivo y se le notificará tal aprobación a la Junta de Directores con copia del reglamento o la política.*

Efecto

Las situaciones comentadas podrían ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias.

La situación comentada en el **apartado a.2** podría ocasionar el incumplimiento de las normas de seguridad con los consiguientes efectos adversos en cuanto a la protección de la información. Esto, a su vez, podría afectar la integridad, disponibilidad y confiabilidad de la información procesada por los usuarios.

Causa

Las situaciones comentadas en los **apartados a.1, a.3, b., c.1, c.3** al **c.6 y d.** obedecen, principalmente, a que el director ejecutivo del Centro Comprensivo en funciones durante el periodo mencionado no le requirió al entonces director de Sistemas de Información que desarrollara y actualizara las normas y los procedimientos escritos de las operaciones de los sistemas computadorizados para su aprobación. Por otro lado, la situación comentada en el **apartado a.2** se atribuye a que el entonces principal oficial financiero no se aseguró de que el director de Sistemas de Información en funciones incluyera las referidas disposiciones ni le requirió a la directora auxiliar de Recursos Humanos que implementara un programa para orientar a todos los empleados del Centro Comprensivo con relación a las normas y los procedimientos de seguridad de la información.

Además, las situaciones comentadas en los **apartados c.2** y **d** obedecen, primordialmente, a la falta de diligencia del principal oficial en funciones, del entonces principal oficial financiero y demás funcionarios concernidos, al no cumplir con las disposiciones de ley y de reglamento, y al no preparar y remitir para la aprobación del director ejecutivo la mencionada reglamentación.

Ver las Recomendaciones 1, 4 y 6.a.10 y 7.c.

Hallazgo 8 – Falta de independencia organizacional del DSI

Situación

La estructura organizacional del Centro Comprensivo no proveía para que la División de Sistemas de Información (DSI) le respondiera a la alta gerencia. El DSI le respondía a la administración del hospital, que era uno de los usuarios del Centro Comprensivo. Además, otros empleados del DSI les respondían a directores de otras divisiones[5], que también eran usuarios de la mencionada División. Dicha estructura no cumplía con el requisito de independencia organizacional que debe prevalecer entre el DSI y sus usuarios.

El 15 de junio de 2018, el entonces director de la Oficina de Gerencia y Presupuesto respondió, mediante carta, a una solicitud de evaluación para la oficialización de la estructura organizacional del Centro Comprensivo. En la misma les recomendó una estructura que proveería una guía clara para mejorar las funciones que debe realizar el Centro Comprensivo e integra algunos cambios a las denominaciones de las unidades, los cuales buscan establecer una comunicación más clara en términos gerenciales. Conforme con dicha estructura, el DSI cumpliría con el requisito de independencia organizacional antes mencionado. No obstante, al 20 de septiembre de 2020, no se había modificado la estructura organizacional del Centro Comprensivo y el DSI no le respondía a la alta Gerencia.

Criterio

El plan de organización es la base sobre la cual funcionan las operaciones en una entidad. En dicho plan se establece, entre otras cosas, la coordinación que debe existir entre las distintas dependencias de la entidad. El DSI debe ser independiente de las oficinas a las que sirve solamente debe responder a los niveles gerenciales más altos.

Efecto

La referida situación puede propiciar que se afecten los servicios de otros departamentos usuarios, lo que, además, podría afectar el desarrollo de otras aplicaciones y ocasionar el estancamiento en el desarrollo de las operaciones del DSI.

---

[5] Un administrador de base de datos y un analista programador recibían supervisión directa del director de Ciencias Poblacionales, el director corporativo de Sistema de Información (puesto vacante), otro administrador de base de datos y un especialista en sistemas de información dedicados al área de Investigación y Radioterapia recibían supervisión directa del oficial principal financiero y de operaciones (también director de Finanzas) y un administrador de sistemas y redes y otro administrador de base de datos respondían directamente a la administradora del Hospital.

Causa

Dicha situación se debía, en parte, a que los entonces directores ejecutivos no habían considerado clasificar a la DSI como una unidad independiente de sus usuarios.

Ver las recomendaciones 1, 4 y 5.

COMENTARIO ESPECIAL

Ausencia de inventarios anuales de la propiedad

En esta sección se comentan situaciones que necesitan ser atendidas, las cuales podrían representar violaciones de ley y de reglamento, que son importantes para las operaciones de la entidad revisada y afectan negativamente al erario.

Situación

El Centro Comprensivo cuenta con una oficina de Propiedad compuesta por un encargado de la propiedad, responsable de: la propiedad; su recibo; distribución; inventario; registro; decomiso; entre otros. Además, tiene la responsabilidad de mantener al día todos los expedientes e inventario de la propiedad aun cuando ésta se encuentre bajo la custodia de otros funcionarios o empleados del Centro Comprensivo.

El examen realizado reveló que, al 12 de agosto de 2020, la Oficina de Propiedad no había preparado los informes de inventario correspondientes a los años fiscales del 2018-19 al 2019-2020. Tampoco el DSI había realizado los inventarios parciales conforme lo establece la *Política Para el Control y Disposición de la Propiedad Mueble e Inmueble* del propio Centro Comprensivo.

Criterio

La situación comentada es contraria a lo establecido en la *Sección 8.6, Normas a seguir para la toma de inventarios por el Encargado de la Propiedad, Incisos 1* y *4* de la *Política Para el Control y disposición de la Propiedad Mueble e Inmueble* aprobada por el entonces director ejecutivo el 24 de septiembre de 2012, la cual establece que:

1. *El Encargado de la Propiedad hará inventario de la propiedad /equipo de cada división u oficina.*
4. *Los inventarios se harán una vez al año; no obstante, el Encargado de la Propiedad realizará inventarios parciales tantas veces como sea necesario para verificar que se están observando las disposiciones de esta Política Institucional. (Política Para el Control y disposición de la Propiedad Mueble e Inmueble, 2012, P.13).*

La situación comentada también es contraria a lo dispuesto en la *Sección 7.2, Directores de Oficina o División, Inciso 8* de la referida Política, la cual establece que:

> *Será responsable de hacer los inventarios físicos parciales de toda la propiedad / equipo asignada al personal bajo supervisión y entregar al Encargado de la Propiedad el inventario certificado. (Política Para el Control y disposición de la Propiedad Mueble e Inmueble, 2012, P.6).*

Efecto

La situación comentada impidió al Centro Comprensivo mantener un control adecuado sobre la propiedad mueble. Esto pudo propiciar la comisión de errores o irregularidades. Además, aumenta el riesgo de pérdida, hurto o uso indebido de la propiedad y dificulta fijar responsabilidades en caso de que ocurran.

Causa

La situación comentada se atribuye a que el encargado de la propiedad había renunciado el 6 de octubre de 2018 y no fue hasta el 3 de marzo de 2020, que se ocupó la vacante. Por otro lado, el puesto de director de sistemas de información estaba vacante desde el 18 de julio de 2018.

Ver las recomendaciones 4 y 9.

COMUNICACIÓN GERENCIAL

Las situaciones comentadas en este *Informe* y otras situaciones determinadas durante el examen fueron discutidas con la directora ejecutiva y el subdirector ejecutivo, en funciones, mediante reunión virtual el 30 de octubre de 2020. En la referida reunión la directora ejecutiva solicitó tiempo para emitir comentarios sobre las situaciones comentadas.

En comunicación recibida mediante correo electrónico, el 6 de noviembre de 2020, el subdirector ejecutivo expresó que no emitirían comentarios al borrador de informe y estarían esperando recibir el informe final para implementar su plan de acción correctiva, conforme a los hallazgos y recomendaciones emitidas por la Oficina del Inspector General.

RECOMENDACIONES

A la junta de directores del Centro Comprensivo

1. Asegurar que la directora ejecutiva cumpla con las recomendaciones de la **3** a la **9**. **(Ver Hallazgos 1 al 8)**

2. Asegurar que la directora ejecutiva le notifique, con copia, la aprobación de un:

a. Informe de Análisis de riesgos de los sistemas de información computarizados, de un análisis de impacto de la entidad, de un plan de manejo de incidentes, de un plan de manejo de emergencias y de un programa de comunicación de crisis. **(Hallazgo 1)**

b. Plan de continuidad de negocios y un plan de recuperación de desastres sobre los sistemas de información. **(Hallazgo 2)**

c. Programa de concientización y adiestramiento y de un programa de pruebas y ejercicios para la continuidad del Centro Comprensivo. **(Hallazgo 3)**

A la directora ejecutiva del Centro Comprensivo

3. Realizar y documentar los análisis de riesgos de los sistemas de información computadorizados y de impacto de negocios, según se establece en las *políticas ATI-003* y *ATI-015*, y que los mismos sean remitidos para su revisión y aprobación. Una vez aprobados, ver que estos se revisen cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Centro Comprensivo para asegurarse de que se mantengan actualizados. **(Hallazgo 1-a. y b.)**

4. Asegurar que el subdirector ejecutivo cumpla con las recomendaciones de la **6** a la **9,** según corresponda. (**Ver hallazgos 1 al 8 y Comentario Especial**)

5. Establecer la División de Sistemas de Información en la estructura organizacional como una unidad independiente de sus usuarios y que le responda a un funcionario de la alta gerencia del Centro Comprensivo. **(Hallazgo 8)**

Al subdirector ejecutivo

6. Impartir instrucciones a la administradora del Hospital para que ejerza una supervisión eficaz sobre el gerente de Sistemas de Información para asegurarse de que identifique alternativas costo-efectivas para preparar y remitir para la aprobación de la directora ejecutiva:

a. El Plan para el Manejo de Incidentes del Centro Comprensivo. Como parte de dicho procedimiento, se debe requerir que se documenten todos los incidentes y cómo se resolvieron, de manera que, cuando estos se repitan, se puedan solucionar en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones. **(Hallazgo 1-c.)**

b. El Programa de Manejo de Emergencias del Centro Comprensivo el cual deberá ser elaborado e implantado conforme a las prácticas profesionales de continuidad establecidas por el *Disaster Recovery Institute International (DRII)*. **(Hallazgo 1-d.)**

c. El Programa de Comunicación de Crisis del Centro Comprensivo en base a las prácticas profesionales de continuidad establecidas por el *Disaster Recovery Institute International*

(DRII). Como parte de dicho programa se deberá: asignar los portavoces oficiales de la agencia, definir los medios de comunicación (prensa, radio, revisión, entre otros), establecer guías para enfrentar situaciones adversas y para asegurarse de que todo el personal y los portavoces estén familiarizados con los procedimientos básicos de comunicaciones y su rol ante la eventualidad de una crisis. **(Hallazgo 1-e.)**

d. El plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones que cumpla con lo requerido en las políticas ATI-003 y ATI-015 de la Carta Circular 140-16. Este plan debe ser remitido ante la consideración de la Junta. Una vez sea revisado y aprobado, asegurarse de que se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios del Centro Comprensivo. Además, asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar su efectividad. **(Hallazgo 2-a.)**

e. Prepare un plan de contingencias o de recuperación de desastres que incluya los aspectos comentados en el **Hallazgo 2-b** y las estrategias de respuestas, recuperación, reanudación y de restauración para todos los procesos críticos del Centro Comprensivo tanto a nivel de las plataformas de procesamiento y de sus comunicaciones. Las estrategias de continuidad establecidas por el Centro Comprensivo estarán basadas en los tiempos de recuperación y resguardo de sus procesos críticos obtenidos en el informe del Análisis de Impacto.

f. Identifique un centro alterno que no esté expuesto a los mismos riesgos que el área de sistemas de información, y que cuente con la infraestructura y los equipos necesarios para restaurar las operaciones críticas computadorizadas del Centro Comprensivo en caso de emergencia. **(Hallazgo 2-c.)**

g. El Programa de Concientización y Adiestramiento y el Programa de Pruebas y Ejercicios que cumplan con lo requerido en la política ATI-015 de la Carta Circular 140-16. **(Hallazgo 3-a. y b.)**

h. Enmiende el *Computer Management Procedure* para evitar situaciones como las que se comentan en el **Hallazgo 6**. Dicho Procedimiento debe contener disposiciones que les requieran a los directores y supervisores de área completar, en todas sus partes, el formulario Solicitud de Acceso a los Sistemas de Información cada vez que éstos soliciten acceso a los recursos de la red para su personal.

i. Verifique que los formularios para solicitar acceso a las redes de comunicaciones sean completados debidamente antes de crear las cuentas que sean solicitadas. **(Hallazgo 6)**

j. Revise y remita para la aprobación de la directora ejecutiva las políticas y procedimientos mencionados, de manera que representen la realidad de las operaciones del Centro

Comprensivo e incluya disposiciones como las mencionadas en los hallazgos 7-a.1, a.3, b., c.1 al c.6 y d.

7. Impartir instrucciones a la directora asociada de Recursos Humanos para que se asegure de que:

   a. se evalúe asignar las funciones, se adiestre y certifique al gerente de sistemas de información y/o administrador de sistemas y redes o se incluya dentro del Plan de Clasificación de Puesto del Centro Comprensivo la clase de Oficial de Seguridad Informática, Gerente de Seguridad Informática, Especialista en Seguridad Informática o sus equivalentes. Una vez creada la referida clase, se reclute el candidato con la educación, experiencia y adiestramiento que lo cualifiquen como experto en seguridad conforme lo establece la Política Núm. ATI-014. **(Hallazgo 4-a.)**

   b. los empleados de la División de Sistemas de Información reciban los adiestramientos necesarios para realizar las funciones que le fueron asignadas. **(Hallazgo 5-a.)**

   c. se establezca un programa de capacitación, en coordinación con la División de Sistemas de Información, para orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información del Centro Comprensivo y dar a conocer la reglamentación y las políticas relacionadas con la seguridad de la información. **(Hallazgos 5-b. y 7-a.2.)**

8. Realizar las gestiones para formalizar los acuerdos que sean necesarios para la utilización del lugar identificado como centro alterno. Dichos acuerdos deben estipular, entre otras cosas, las necesidades y los servicios requeridos para afrontar una emergencia, y el lugar o los lugares donde podrían ser requeridos dichos servicios. Por el contrario, considerar establecer su propio centro alterno en alguna de sus instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la DSI. **(Hallazgo 2-c)**

9. Impartir instrucciones al director de Finanzas o su representante, para que, ejerza una supervisión efectiva sobre el Encargado de la Propiedad, de manera de, que se asegure de que se realicen los inventarios anuales de la propiedad. **(Comentario Especial 1) y cumplir con la Carta Circular 2021-01, de 8 de marzo de 2021, de la Oficina del Inspector General de Puerto Rico.**

CONCLUSIÓN

La evaluación realizada a los documentos, y la información recopilada durante este examen, revelaron los **hallazgos y deficiencias de controles internos según** detallados, para los cuales e emiten las correspondientes recomendaciones. Sera responsabilidad de la gerencia, corregir las

deficiencias y establecer los controles internos efectivos para asegurar el buen funcionamiento y operación de los sistemas de información en el Centro Comprensivo de Cáncer.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017, según enmendada, hoy 14 de mayo de 2021, en San Juan, Puerto Rico.

Ivelisse Torres Rivera
Inspectora General

INFORMACIÓN GENERAL

Misión

Consolidar los recursos y esfuerzos del Gobierno de Puerto Rico, para promover una sana administración pública y mediante una preintervención efectiva, el óptimo funcionamiento de sus instituciones.

Visión

Servir como entidad gubernamental reconocida a nivel local e internacional y lograr a través de auditorías internas y acciones preventivas, el funcionamiento efectivo y eficiente d ellos fondos y de la propiedad pública del Gobierno de Puerto Rico.

Línea de Consultas

La Oficina del Inspector General tiene el compromiso de promover una sana administración pública. Por lo que, cualquier persona que tenga información sobre un acto irregular o falta de controles internos en las operaciones de la rama ejecutiva, puede comunicarse a la OIG a través de:

- Línea de Consultas: 787-679-7979
- Correo Electrónico: informa@oig.pr.gov

Contactos


PO box 191733 San Juan, Puerto Rico 00919-1733


Ave Arterial Hostos 249 Esquina Chardón Edificio ACAA Piso 7, San Puerto Rico 00918


787-679-7997


consultas@oig.pr.gov


www.oig.pr.gov