INFORME DE AUDITORÍA TI-17-08

13 de marzo de 2017

Comisión Apelativa del Servicio Público

Sistemas de Información Computadorizados

(Unidad 5344 - Auditoría 14028)

Período auditado: 15 de julio de 2015 al 15 de enero de 2016

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **5**

OPINIÓN Y HALLAZGOS **6**

1 - Falta de un informe de análisis de riesgos, de un análisis de impacto de negocio y de un procedimiento para el manejo de incidentes 6

2 - Falta de un plan de continuidad de negocios, de un plan de contingencias sobre los sistemas de información, y de un centro alterno para la recuperación de las operaciones computadorizadas 8

3 - Falta de normas y procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados de la Comisión, de actualización del Reglamento sobre equipo computadorizado y servicios relacionados, y de las políticas sobre el uso de los sistemas de información 12

4 - Falta de controles físicos en las áreas de distribución de cableado 15

5 - Deficiencias relacionadas con los parámetros de seguridad, y falta de revisiones periódicas de los registros producidos por el sistema operativo 17

6 - Deficiencias relacionadas con el manejo, almacenamiento y control de los respaldos de información, y falta de pruebas de restauración de los respaldos 20

RECOMENDACIONES **24**

AGRADECIMIENTO **27**

ANEJO 1 - COMISIONADOS ASOCIADOS DURANTE EL PERÍODO AUDITADO **28**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **29**

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

13 de marzo de 2017

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

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 15 de julio de 2015 al 15 de enero de 2016. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene seis hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, el acceso y la continuidad del servicio de la Comisión. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Comisión se creó en virtud del *Plan de Reorganización 2 de 26 de julio de 2010, Plan de Reorganización de la Comisión Apelativa del Servicio Público*. Dicho *Plan*, creado al amparo de la *Ley 182-2009, Ley de Reorganización y Modernización de la Rama Ejecutiva del Gobierno de Puerto Rico de 2009*, según enmendada, y que entró en vigor el 24 de noviembre de 2010, fusionó la Comisión Apelativa del Sistema de Administración de Recursos Humanos del Servicio Público (CASARH) y la Comisión de Relaciones del Trabajo del Servicio Público (CRTSP).

La Comisión es un organismo cuasijudicial especializado en asuntos obrero-patronales y del principio de mérito. En esta se atienden casos laborales, de administración de recursos humanos y de querellas de los empleados públicos cubiertos por la *Ley 45-1998, Ley de Relaciones del Trabajo para el Servicio Público de Puerto Rico*, y por la *Ley 184-2004, Ley para la Administración de los Recursos Humanos en el Servicio Público del Estado Libre Asociado de Puerto Rico*, según enmendadas; que sean empleados de los municipios o ciudadanos que aleguen que una acción o determinación le afecta su derecho de competir o ingresar al Sistema de Administración de los Recursos Humanos, de conformidad al principio de mérito.

La Comisión también atiende las querellas conforme a lo dispuesto en la *Ley 333-2004, Carta de Derechos de los Empleados Miembros de una Organización Laboral*, según enmendada, en los casos de empleados y organizaciones laborales o asociaciones llamadas *bona fide*, creadas al amparo de la *Ley Núm. 134 de 19 de julio de 1960, Cuotas de Agrupaciones de Servidores Públicos*, y de la *Ley Núm. 139 de 30 de junio de 1961, Cuotas de Agrupaciones de Empleados Municipales*, según enmendadas; y de aquellas otras organizaciones laborales no comprendidas bajo la *Ley Núm. 130 de 8 de mayo de 1945, Ley de Relaciones del Trabajo de Puerto Rico*, según enmendada. A su vez, la Comisión busca desarrollar e implementar políticas públicas en torno a la organización de empleados en sindicatos en el sector público.

Entre los objetivos de la Comisión están atender los casos de relaciones obrero-patronales y de administración de recursos humanos del servicio público bajo un mismo foro adjudicativo especializado para reducir gastos al erario; interpretar, aplicar y hacer cumplir la política pública en torno a la negociación colectiva en el sector público; uniformar los procesos decisionales y las normas de adjudicación de controversias en el sector público; garantizar que tanto la administración de recursos humanos como el sistema de relaciones laborales en el sector público estén predicados en el principio de mérito, de modo que se proteja el derecho de los empleados y ciudadanos sobre la base de no discrimen por razón de raza, color, sexo, religión, nacimiento, origen o condición social, ideas religiosas, ideas políticas, edad, condición de veterano, condición física o mental; y proteger la prevalencia de los derechos de los empleados públicos miembros de organizaciones laborales.

La Comisión está compuesta por 1 presidente y 6 comisionados asociados, los cuales son nombrados por el Gobernador de Puerto Rico con el consejo y consentimiento del Senado de Puerto Rico. El Presidente y 3 de los comisionados deben ser abogados admitidos al ejercicio de la profesión y todos los comisionados asociados, incluido el Presidente, deben tener vasto conocimiento y experiencia en el campo de la administración de los recursos humanos, y en la aplicación y la defensa del principio de mérito en las relaciones obrero-patronales. Todos los nombramientos serán por términos de 10 años a partir de la fecha de vencimiento del término anterior.

Para realizar sus funciones, la Comisión cuenta con las oficinas del Presidente, de los Comisionados Asociados, y de Asuntos Administrativos; y con las divisiones de Investigación, de Métodos Alternos de Resolución de Conflictos, de Secretaría y Legal.

La Comisión tiene una infraestructura tecnológica que consta de 9 servidores, de los cuales 1 es virtual, 10 *switches*[1], y 64 computadoras conectadas a la red. Además, cuenta con 1 red de área local (*LAN*, por sus siglas en inglés) y 1 línea dedicada a Internet que da servicio a sus divisiones

[1] Dispositivo de comunicación central que conecta dos o más segmentos de red y permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

y oficinas ubicadas en los 2 pisos del edificio. Los sistemas de información computadorizados de la Comisión son administrados por el Programador de Sistemas de Información (Programador), quien responde al Presidente.

Los recursos para financiar las actividades operacionales de la Comisión provienen de la Resolución Conjunta del Presupuesto General. El presupuesto asignado a la Comisión, para los años fiscales del 2013-14 al 2015-16, ascendió a $3,632,910, $3,480,490 y $3,244,000, respectivamente.

Los **anejos 1 y 2** contienen una relación de los funcionarios principales de la Comisión que actuaron durante el período auditado.

La Comisión cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.casp.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Lcdo. Laudelino F. Mulero Clas, Presidente de la Comisión, mediante cartas de nuestros auditores del 10 de noviembre de 2015 y del 10 de febrero de 2016. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 4 de diciembre de 2015 y 29 de febrero de 2016, el Presidente remitió sus comentarios, los cuales fueron considerados en la redacción del borrador de este *Informe*.

El borrador de ocho hallazgos se remitió para comentarios al Presidente mediante carta del 16 de noviembre de 2016. En este borrador se indicaron datos específicos, tales como: la ubicación, la descripción y los números de propiedad de equipos computadorizados, y los nombres de servidores, los cuales, por seguridad, no se incluyen en este *Informe*.

El 29 de noviembre de 2016 el Presidente solicitó una prórroga para remitir sus comentarios, la cual le concedimos hasta el 9 de enero de 2017. Ese día solicitó una prórroga adicional la cual concedimos hasta el 31 de enero.

El Presidente contestó el borrador mediante correo electrónico del 31 de enero. Luego de evaluar sus comentarios y la evidencia suministrada,

determinamos que la Comisión tomó las acciones correctivas pertinentes, excepto por los **hallazgos** que se incluyen en este *Informe*. En los mismos se incluyeron algunos de sus comentarios.

OPINIÓN Y HALLAZGOS

Opinión favorable con excepciones

Las pruebas efectuadas revelaron que las operaciones de los sistemas de información computadorizados de la Comisión, en lo que concierne a los controles establecidos para la administración del programa de seguridad, el acceso y la continuidad del servicio, se realizaron sustancialmente de acuerdo con las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos, de un análisis de impacto de negocio y de un procedimiento para el manejo de incidentes

Situaciones

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en una entidad, sus vulnerabilidades y las amenazas a las que se encuentran expuestos, así como 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.

   Al 17 de agosto de 2015, en la Comisión no se había preparado un informe del análisis de riesgos de los sistemas de información computadorizados.

b. El análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por la pérdida o la interrupción de las operaciones, y de las vulnerabilidades y las amenazas que fueron identificadas y clasificadas en el análisis de riesgos. Además, debe

proveer información para determinar las estrategias de recuperación más apropiadas. Al 17 de agosto de 2015, en la Comisión no se había realizado un análisis de impacto de negocio sobre los sistemas de información computadorizados.

c. Al 29 de septiembre de 2015, la Comisión no tenía un procedimiento o plan para el manejo de incidentes que 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.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*[2], aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto (OGP); y en la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el Director de la OGP.

Efectos

Las situaciones comentadas en los **apartados a. y b.** impiden a la Comisión estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificultan desarrollar un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones de la Comisión, en caso de que surja alguna eventualidad. **[Véase el Hallazgo 2-a.]**

[2] Dicha *Carta Circular* fue derogada por la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el Director de la OGP. Esta contiene disposiciones similares a las de la *Carta Circular* derogada.

La situación comentada en el **apartado c.** le impide a la Comisión 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.

Causas

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a que, según el Presidente, los empleados de la Comisión conocían los riesgos y el impacto que ocasionaría la pérdida de equipo o la interrupción en las operaciones de la agencia, pero no lo habían documentado para su aprobación. Tampoco 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 *TIG-003* y *TIG-015*.

La situación comentada en el **apartado c.** se atribuye a que el Presidente no había impartido directrices al Programador para el desarrollo y la aprobación del procedimiento para el manejo de incidentes.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, que están en el proceso de preparación de los informes de análisis de riesgos y de impacto de negocio, y del plan para el manejo de incidentes asociados a los sistemas de información computadorizados.

Véanse las recomendaciones 1 y 2.a.1).

Hallazgo 2 - Falta de un plan de continuidad de negocios, de un plan de contingencias sobre los sistemas de información, y de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Al 17 de noviembre de 2015, la Comisión 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 de la

Comisión, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. Al 9 de noviembre de 2015, la Comisión carecía de un plan de contingencias que incluyera los siguientes requisitos para atender situaciones de emergencia:

- Los procedimientos a seguir cuando el centro de cómputos 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 de la Comisión
- 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 nombre 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 29 de septiembre de 2015, la Comisión 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 esta.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

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 convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios 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 propia entidad.

Efectos

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 de la Comisión.

La situación comentada en el **apartado c.** podría afectar las operaciones de la Comisión, 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 de la Comisión.

Causas

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 de la Comisión 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. **[Véase el Hallazgo 1-a.]**

La situación comentada en el **apartado c.** se atribuye a que el Presidente de la Comisión no le había requerido al Programador que realizara las gestiones necesarias para identificar un lugar disponible y adecuado como centro alterno para formalizar los acuerdos necesarios para la utilización del mismo en casos de emergencia.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, que están en el proceso de la preparación de los planes de continuidad de negocios y de contingencias asociados con los sistemas de información computadorizados. **[Apartados a. y b.]**

Además, nos informó de las medidas que están en proceso de implementar para corregir la situación comentada en el **apartado c.**

Véanse las recomendaciones 2.a.2) y 3), b., y 3.

Hallazgo 3 - Falta de normas y procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados de la Comisión, de actualización del Reglamento sobre equipo computadorizado y servicios relacionados, y de las políticas sobre el uso de los sistemas de información

Situaciones

a. Al 16 de septiembre de 2015, en la Comisión no se habían promulgado normas ni procedimientos escritos para reglamentar lo siguiente:

- La administración y el control de los accesos lógicos y físicos de los recursos de tecnología de información
- El otorgamiento, la modificación o la cancelación del acceso local y remoto a los usuarios
- La instalación y modificación del sistema operativo de las computadoras
- La instalación y configuración de la red de comunicaciones
- El mantenimiento al equipo, y la administración y documentación de los problemas y cambios, de manera que se prevengan las interrupciones no esperadas
- La adquisición de aplicaciones computadorizadas.

b. Al 15 de julio de 2015, la Comisión contaba con dos reglamentos relacionados con los sistemas de información computadorizados:

- *Orden Administrativa 03-2002, Reglamento sobre equipo computadorizado y servicios relacionados*, aprobado el 1 de julio de 2002 por el Presidente de la CRTSP
- *Orden Administrativa 01-2006, Políticas sobre el uso de los sistemas de información*, aprobada el 10 de febrero de 2006 y enmendada por la *Orden Administrativa 2008-03* aprobada el 11 de marzo de 2008 por la Presidenta de la CASARH.

La Comisión había adoptado estas órdenes administrativas a partir de la fusión de estas agencias conforme al *Plan de Reorganización 2*.

El examen efectuado el 26 de octubre de 2015 a estas órdenes administrativas reveló que no habían sido revisadas para atemperarlas a las operaciones de la Comisión, según se indica:

1) Relacionado con la *Orden Administrativa 03-2002*:

   - Se menciona el programa *Trabajo de Verano para los Hijos de los Empleados* y en la Comisión no existe dicho programa.
   - Se indica que, cuando el empleado necesita utilizar equipo de trabajo remoto, este debe completar el *Permiso de Uso de Laptop*. A la fecha del examen, los empleados de la Comisión utilizaban computadoras de escritorio, por lo que este formulario no era necesario.
   - Se indica que las contraseñas serán renovadas cada 180 días, cuando el servidor principal está configurado para que se cambien cada 120 días.
   - Se establece que los usuarios pueden acceder la red de lunes a viernes de 6:00 a.m. a 10:00 p.m. Actualmente, el período para acceder la red está configurado en el servidor de 6:00 a.m. a 7:00 p.m.

2) Las órdenes administrativas *01-2006* y *2008-03* hacen referencia a una oficina de sistemas de información. La Comisión no cuenta con una oficina de sistemas de información. Los servidores y demás equipos se mantienen en la oficina del Programador.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Artículo 9.e) del *Plan de Reorganización 2*. En este se indica que el Presidente tendrá la facultad de aprobar la reglamentación administrativa necesaria para viabilizar un eficaz y adecuado funcionamiento de la Comisión.

Además, son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que será responsabilidad de cada entidad gubernamental desarrollar normas específicas que consideren las

características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Esto implica, como norma de sana administración, establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y estén actualizados y aprobados por la alta gerencia y que sean uniformes. Mediante los mismos, se logra 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 facilita la labor de adiestramiento.

Efectos

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. Además, podría exponer al personal de sistemas de información, a los equipos y a la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

Causa

Las situaciones comentadas obedecen, principalmente, a que el Presidente de la Comisión no le requirió al Programador que desarrollara y actualizara las normas y los procedimientos escritos de las operaciones de los sistemas computadorizados para su aprobación.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, que están en el proceso de preparar las normas y los procedimientos mencionados en el **apartado a.**, y de revisar y actualizar el reglamento y las políticas indicados en el **apartado b.**

Véase la Recomendación 2.a.4).

Hallazgo 4 - Falta de controles físicos en las áreas de distribución de cableado

Situaciones

a. La Comisión contaba con 6 áreas en las que estaban localizados 10 *switches* que mantenían las conexiones necesarias para interconectar las computadoras que recibían servicio de la red. El examen efectuado el 7 y 21 de agosto de 2015 a los controles físicos[3] de estas áreas, reveló que no existían condiciones de seguridad adecuadas para proteger los equipos de comunicación de la Comisión e impedir que personal no autorizado pudiera tener acceso a los mismos, según se indica:

   1) En dos de las áreas, los *switches* se encontraban en la parte posterior de las fotocopiadoras, lo que los hacía vulnerables a daños por el movimiento de estas. Esta situación se agravaba debido a que estaban ubicados cerca del piso, lo que los hacía vulnerables al polvo, la humedad y la posibilidad de que los pisaran y fueran desconectados por las personas que utilizaban las fotocopiadoras.

   2) En dos de las áreas, los *switches* estaban ubicados en la pared y los cables estaban expuestos, lo que los hacía vulnerables a daños involuntarios o intencionales.

   3) En dos de las áreas, los *switches* se encontraban sobre unos escritorios, lo que los hacía vulnerables, ya que podían caerse y romperse o desconectarse los equipos.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los

[3] Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados, por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Esto implica que, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso a las áreas donde están ubicados los servidores y los equipos de comunicaciones
- Se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas
- Los equipos periféricos deben ser cuidados y utilizados correctamente para evitar averías causadas por accidentes.

Efectos

Las situaciones comentadas podrían facilitar que personas no autorizadas tuvieran acceso a los equipos de comunicación, lo que representa un riesgo para la continuidad de los servicios que ofrece la Comisión, así como la confidencialidad de la información. Además, pudieran ocasionar daños y deterioros prematuros a los *switches*, lo que podría impedir el obtener el rendimiento máximo en términos de los servicios que estos ofrecen.

Causa

Las situaciones comentadas se debieron a que el Programador no había establecido los controles de seguridad y de acceso físico para proteger los *switches* y sus conexiones.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, las medidas que están en proceso para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 2.c.

Hallazgo 5 - Deficiencias relacionadas con los parámetros de seguridad, y falta de revisiones periódicas de los registros producidos por el sistema operativo

Situaciones

a. La Comisión contaba con nueve servidores para llevar a cabo sus operaciones y brindar sus servicios. El examen efectuado el 16 de noviembre de 2015 sobre los parámetros de seguridad definidos en el sistema operativo del servidor principal[4] de la Comisión reveló que no estaban definidas:

   1) Las políticas de auditoría (*Audit Policy*) para que el sistema produjera un registro sobre los eventos relacionados con el uso de los privilegios asignados a los usuarios (*Audit privilege use*) y las acciones ejecutadas por algún programa (*Audit process tracking*).

   2) Las políticas sobre los privilegios asignados a los usuarios (*User Rights Assignment*) ni las opciones de seguridad (*Security Options*).

   3) Las opciones de seguridad para lo siguiente:

      - Desactivar automáticamente la cuenta del usuario una vez venciera el término de acceso a los recursos de la red, previamente establecido a nivel del sistema operativo (*Do not force logoff when logon hours expire)*. En su lugar, el Programador definía el horario de acceso a nivel de usuario, o sea, individualmente en cada una de las cuentas.

      - Requerirle al usuario entrar una contraseña para continuar con el uso de la red, luego de un período de inactividad (*Idle time before suspending session*).

b. Para acceder a los recursos de sistemas de información, la Comisión contaba con un servidor principal que permitía el acceso a la red, y otro que permitía el acceso a Internet a los usuarios autorizados.

[4] Este servidor es el que controla el proceso de autenticación para permitir o denegar los accesos a los recursos del dominio.

Para el correo electrónico, la Comisión utilizaba el servicio de *Office 365,* obtenido a través de un contrato global de licenciamiento entre *Microsoft* y la OGP. Mediante este contrato, se provee un dominio individual a cada agencia, la cual es responsable de la administración y creación de sus cuentas de acceso.

Al 8 de diciembre de 2015, el Programador no examinaba periódicamente los registros de seguridad producidos por el sistema operativo sobre el acceso a los sistemas de información computadorizados, y sobre el uso de Internet y del correo electrónico. Esto, 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. El Programador revisaba estos eventos sólo cuando ocurrían situaciones de emergencia.

Criterios

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades gubernamentales deberán 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. Esta norma se establece, en parte, mediante lo siguiente:

- La activación de todas las opciones para registrar los eventos de seguridad del sistema operativo **[Apartado a.1) y 2)]**
- La limitación del tiempo de acceso para todas las cuentas de acceso de acuerdo con las funciones de cada usuario **[Apartado a.3)]**
- El uso de todas las opciones para restringir y controlar los accesos que provee el sistema operativo del servidor principal. **[Apartado a.3)]**

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las entidades gubernamentales deberán establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que estos proveen. Además, la agencia puede reservarse el derecho a intervenir y auditar los accesos realizados por los usuarios mediante el acceso a la red, a Internet y

al correo electrónico. Esta norma se establece, en parte, mediante el examen continuo de las bitácoras (*logs*) que provee cada herramienta en las que se detallan los accesos de los usuarios a los sistemas de información computadorizados y la información accedida.

Efectos

Las situaciones comentadas en el **apartado a.1)** impiden a la Comisión mantener un registro de los eventos inusuales o los problemas ocurridos en la red que le permitiera al Programador tomar a tiempo las medidas correctivas o preventivas necesarias.

Lo comentado en el **apartado a.2) y 3)** propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y 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 detectadas a tiempo para fijar responsabilidades. Además, relacionado con el **apartado a.3)**, configurar los horarios a nivel de usuario ocasiona que, al expirar las horas establecidas, este pueda mantener abierta una sesión.

La falta de verificaciones periódicas de las bitácoras que provee el sistema operativo priva a la Comisión de las herramientas necesarias para detectar irregularidades y alteraciones, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados sin que se puedan detectar a tiempo para fijar responsabilidades. **[Apartado b.]**

Causas

Las situaciones comentadas se debieron a que el Programador no se había puesto en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo. **[Apartado a.]**

La situación comentada el **apartado b.** se debía a que:

- El Presidente de la Comisión no había impartido instrucciones al Programador para que este revisara periódicamente las bitácoras de acceso a los sistemas de información computadorizados

- El Programador, al ser el único empleado del área de sistemas de información, realizaba todas las funciones relacionadas con los sistemas de información computadorizados de la Comisión. Por esto, se le hacía difícil la revisión periódica de los registros de seguridad.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, que las situaciones comentadas en el **apartado a.** fueron corregidas. Sin embargo, no nos suministraron la evidencia de las correcciones efectuadas.

Además, el Presidente de la Comisión nos indicó las medidas que están en proceso para corregir la situación comentada en el **apartado b.**

Véase la Recomendación 2 de la d. a la f.

Hallazgo 6 - Deficiencias relacionadas con el manejo, almacenamiento y control de los respaldos de información, y falta de pruebas de restauración de los respaldos

Situaciones

a. Al 23 de septiembre de 2015, la Comisión contaba con nueve servidores en el área donde se ubican los sistemas de información, en los que se mantenían bases de datos, correspondencia y documentos almacenados en la red. El Programador realizaba respaldos diarios a los siguientes servidores:

   - A dos servidores se les realizaba un respaldo incremental automático, mediante el programa provisto para esto en el sistema operativo *Windows Server 2003*, instalado en los mismos.
   - A un servidor se le realizaba un respaldo del *Bare Metal Recovery*[5], del *System State*[6] y de las particiones C: y F:
   - A un servidor se le realizaba un respaldo del *Bare Metal Recovery*, del *System State* y de la partición C:
   - A un servidor se le realizaba un respaldo completo (*full backup*).

[5] Este respaldo incluye el sistema operativo, y las aplicaciones y los datos necesarios para la recuperación y restauración del sistema respaldado.

[6] Este respaldo incluye información de la configuración actual del equipo, tal como: los registros, los archivos de iniciación (*boot files*) y el *active directory*.

- A un servidor se le realizaba un respaldo de los archivos de las grabaciones de las vistas y de unos compartidos (share folders) en la rutina de respaldo incremental de otro servidor
- A un servidor se le realizaba un respaldo a las reglas del *firewall* activas y las inactivas
- A un servidor se le realizaba un respaldo completo y lo incluían en la rutina de respaldo incremental de otro servidor.

Además, todos los primeros viernes de mes se realizaba un respaldo completo en un servidor que luego se transfería al *Network Attached Storage* (NAS)[7], y se grababa en cinta.

La Comisión mantenía un acuerdo colaborativo con una entidad para almacenar y manejar las cintas de respaldo.

En el examen realizado el 28 de octubre de 2015 sobre el proceso de manejo y almacenamiento de los respaldos de información determinamos lo siguiente:

1) En una caja de seguridad en la entidad sólo había una cinta que contenía el respaldo incremental efectuado el 22 de octubre de 2015. Este tipo de respaldo sólo mantiene los archivos que han cambiado desde el último respaldo completo. Al no mantenerse el respaldo completo en la caja de seguridad, no se podría recuperar la información y continuar con las operaciones de la Comisión en caso de una emergencia.

2) En la caja de seguridad de la Comisión encontramos 4 cintas que correspondían al respaldo de agosto de 2015 y 62 cintas a los respaldos diarios incrementales de septiembre y octubre de 2015. No encontramos la cinta de respaldo completo mensual de septiembre de 2015. Este se mantenía en el NAS de la Comisión.

3) La Comisión no mantenía un registro de los respaldos realizados a la información de los servidores ni de las cintas enviadas al centro de almacenamiento externo, en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor

[7] El NAS es una tecnología de almacenamiento de información.

donde se mantienen estos archivos, la última fecha de actualización de información y la explicación de fallas o situaciones especiales que ocurrieron, si alguna, durante la preparación de los respaldos. El registro que llevaban sólo contenía el registro de los acarreos donde se establecía la fecha y la persona encargada de llevar la cinta de respaldo.

b. Al 29 de septiembre de 2015, en la Comisión no se habían realizado pruebas periódicas de restauración de las cintas de respaldo de los sistemas de información computadorizados para verificar que se pueda recuperar la información en caso de una falla de la aplicación o del equipo.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. Conforme a dicha política pública, se requieren procedimientos escritos para mantener una copia de respaldo recurrente de la información y de los programas de aplicación y de sistema, esenciales e importantes para las operaciones. En los mismos se deberá establecer qué información será respaldada, la frecuencia con que se preparará los respaldos y con que se llevarán al sitio alterno, de tener uno. La información sobre la cantidad de respaldos y la frecuencia de su preparación deberá estar basada en el análisis de riesgos de los sistemas de información y, a su vez, en el plan de continuidad de negocios. **[Apartado a.1) y 2)]**

Las mejores prácticas en el campo de la tecnología de información sugieren lo siguiente:

- Como parte integral del plan de continuidad de negocios, toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, debe ser duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, para recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. **[Apartado a.1) y 2)]**

- Se debe mantener un inventario detallado de los medios magnéticos de respaldos para facilitar su localización y para sustituir periódicamente, por medios magnéticos nuevos, los utilizados para los respaldos. **[Apartado a.3)]**
- Se efectúen pruebas periódicas de restauración a los respaldos de información. Esto, para garantizar que la información de los respaldos esté completa y disponible en caso de que ocurra un evento inesperado que requiera la utilización de los mismos. **[Apartado b.]**

Efectos

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

Lo comentado 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 los sistemas en caso de contingencias o emergencias.

La situación comentada en el **apartado b.** podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales y afectar las funciones de la Comisión y sus sistemas de información computadorizados.

Causas

Las situaciones comentadas en el **apartado a.** se debieron a que la Comisión no contaba con un procedimiento para la preparación de los respaldos de la información almacenadas en sus sistemas de información. El que tenían le correspondía a las operaciones de la Comisión de Relaciones del Trabajo del Servicio Público y su sistema de respaldo.

La situación comentada en el **apartado b.** se atribuye a que en la Comisión no se había desarrollado un procedimiento para las pruebas de recuperación de las cintas de respaldo. Tampoco el Presidente le había requerido al Programador a realizar las pruebas indicadas.

Comentarios de la Gerencia

El Presidente de la Comisión nos indicó en su carta, entre otras cosas, las medidas implementadas para corregir la situación comentada en el **apartado a.1) y 2)**. Sin embargo, no se nos suministró evidencia de las correcciones efectuadas.

Además, el Presidente de la Comisión nos indicó las medidas que estaban en proceso para corregir las situaciones comentadas en los **apartados a.3) y b.**

Véase la Recomendación 2 de la g. a la i.

RECOMENDACIONES

Al Presidente de la Comisión Apelativa del Servicio Público

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

2. Ejercer una supervisión efectiva sobre el Programador para asegurarse de que:

    a. Identifique alternativas costo-efectivas para preparar y remitir, para su aprobación:

        1) El procedimiento para el manejo de incidentes. 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.]**

        2) El plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones, según se establece en la *Política TIG-003*. Una vez este sea revisado y aprobado, asegurarse de que se

realicen pruebas periódicas para garantizar la efectividad del mismo, y se divulgue a los empleados y a los funcionarios concernientes. Además, se mantenga una copia del mismo en un lugar seguro fuera de lo predios de la Comisión. **[Hallazgo 2-a.]**

3) Un plan de contingencias que incluya los aspectos comentados en el **Hallazgo 2-b.**

4) Las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 3-a.** Además, de atemperar las órdenes administrativas para que reflejen la realidad de las operaciones de la Comisión. **[Hallazgo 3-b.]**

b. 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 de la Comisión en caso de emergencia. **[Hallazgo 2-c.]**

c. Establezca los controles necesarios para corregir las situaciones indicadas en el **Hallazgo 4**. Esto, de manera que se asegure de que los equipos de comunicación de la Comisión se mantengan en lugares donde estén protegidos contra accesos no autorizados y contra posibles daños causados por condiciones ambientales y físicas, que puedan afectar la confidencialidad de la información, y la disponibilidad y el rendimiento de estos equipos.

d. Evalúe las opciones correspondientes a las políticas de auditorías (*Audit Policy*), los parámetros de seguridad (*Security Options*) y los privilegios a los usuarios (*User Rights Assignment*), y active las que considere necesarias de acuerdo con los riesgos y las amenazas de la Comisión. **[Hallazgo 5-a.1) y 2)]**

e. Se efectúen las modificaciones en los parámetros de seguridad del sistema operativo del servidor principal para:

1) Desconectar automáticamente del sistema a los usuarios, una vez venza el término de acceso a la red establecido. **[Hallazgo 5-a.3)]**

2) Requierir a los usuarios entrar una contraseña para continuar con el uso de la red luego de un período de inactividad. **[Hallazgo 5-a.3)]**

f. Revise y documente las revisiones realizadas a los registros de seguridad del acceso a los sistemas de información computadorizados, a Internet y al correo electrónico, de ser necesario, tome de inmediato las medidas preventivas y correctivas. **[Hallazgo 5-b.]**

g. Prepare copias recurrentes de los respaldos realizados a los servidores y almacenados en el disco externo, las almacene en un lugar fuera de los predios de la Comisión, y mantenga un registro de las mismas. **[Hallazgo 6-a.1) y 2)]**

h. Mantenga un registro de los respaldos que le permita controlar y documentar adecuadamente la preparación de estos. Además, se asegure de que el registro contenga la información que se indica en el **Hallazgo 6-a.3)**.

i. Realice pruebas de recuperación de los respaldos guardados en el NAS y en las cintas, y de los enviados al centro de almacenamiento externo, para validar la efectividad de los mismos. **[Hallazgo 6-b.]**

3. 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. **[Hallazgo 2-c.]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yermín M. Valdivieso

ANEJO 1

COMISIÓN APELATIVA DEL SERVICIO PÚBLICO
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS
COMISIONADOS ASOCIADOS DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Laudelino F. Mulero Clas	Presidente	15 jul. 15	15 ene. 16
Lcda. Carmen R. Lugo Somolinos	Comisionada Asociada	15 jul. 15	15 ene. 16
Lcda. Wanda R. Caldas Díaz	"	15 jul. 15	15 ene. 16
Lcda. Marisol Díaz Guerrero	"[8]	15 jul. 15	30 nov. 15
Lcda. Evelyn D. Reyes Ríos	"	15 jul. 15	15 ene. 16
Sra. Rixie V. Maldonado Arrigoitía	"	15 jul. 15	15 ene. 16
Sr. Héctor A. Santiago González	Comisionado Asociado	15 jul. 15	15 ene. 16

[8] Este puesto estuvo vacante del 1 de diciembre de 2015 al 15 de enero de 2016.

ANEJO 2

COMISIÓN APELATIVA DEL SERVICIO PÚBLICO
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Laudelino F. Mulero Clas	Presidente	15 jul. 15	15 ene. 16
Sr. Carlos M. Bermúdez Torres	Director de Asuntos Administrativos	15 jul. 15	15 ene. 16
Sr. Reynaldo González Rodríguez	Director de la División de Secretaría	15 jul. 15	15 ene. 16
Sr. José A. Rivera Soto	Director de la División de Investigaciones	15 jul. 15	15 ene. 16
Sra. Ihomara A. Quiñonez Reyes	Directora de la División de Métodos Alternos y Resolución de Conflictos	15 jul. 15	15 ene. 16
Lcdo. Urayoán Pérez Alemán	Director de la División Legal	15 jul. 15	15 ene. 16
Sra. Carmen R. Roque Torres	Analista en Administración de Recursos Humanos	15 jul. 15	15 ene. 16
Sr. Javier Ferrer Briones	Programador de Sistemas de Información	15 jul. 15	15 ene. 16

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:
105 Avenida Ponce de León
Hato Rey, Puerto Rico
Teléfono: (787) 754-3030
Fax: (787) 751-6768

Dirección postal:
PO Box 366069
San Juan, Puerto Rico 00936-6069

Internet:
www.ocpr.gov.pr

Correo electrónico:
ocpr@ocpr.gov.pr