INFORME DE AUDITORÍA TI-18-04

1 de marzo de 2018

Junta de Relaciones del Trabajo de Puerto Rico

Sistemas de Información Computadorizados

(Unidad 5349 - Auditoría 14128)

Período auditado: 31 de mayo al 23 de diciembre de 2016

CONTENIDO

Página

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

1 de marzo de 2018

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos a los sistemas de información computadorizados de la Junta de Relaciones del Trabajo de Puerto Rico (Junta). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVO DE AUDITORÍA

Determinar si las operaciones de la Junta, en lo que concierne a los controles internos para la administración del programa de seguridad; el acceso lógico y físico; y la continuidad del servicio, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este *Informe* contiene cinco hallazgos sobre el resultado del examen que realizamos de las áreas indicadas en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 31 de mayo al 23 de diciembre 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. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestros hallazgos y opinión. En consecuencia, realizamos las pruebas que consideramos necesarias, a base

de muestras y de acuerdo con las circunstancias, según nuestro objetivo de auditoría. Realizamos pruebas tales como: entrevistas a funcionarios y a empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o por fuentes externas; pruebas y análisis de procedimientos de control interno, y de otros procesos; y confirmaciones de información pertinente.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Junta fue creada mediante la *Ley Núm. 130 del 8 de mayo de 1945, Ley de Relaciones del Trabajo de Puerto Rico*, según enmendada, para promover los principios de la negociación colectiva, reducir al mínimo las causas de ciertas disputas obreras y fomentar la productividad económica. La Junta es un organismo cuasi-judicial de la Rama Ejecutiva que está facultado para deliberar y adjudicar, mediante decisiones finales, las controversias obrero-patronales que se le remiten, luego de haber sido evaluadas e investigadas por los diferentes componentes de esta agencia. Además, atiende y resuelve las querellas o violaciones relacionadas con la Carta de Derechos de los Empleados Miembros de una Organización Laboral, en los casos de empleados y organizaciones laborales del sector público bajo su jurisdicción conforme a la *Ley Núm. 130*. También tiene jurisdicción primaria exclusiva para atender apelaciones surgidas como consecuencia de acciones o decisiones tomadas conforme al *Capítulo II de la Ley 66-2014, Ley de Sostenibilidad Fiscal y Operacional del Estado Libre Asociado de Puerto Rico*, de aquellos empleados cubiertos por la *Ley Núm. 130*.

Su función principal es proteger los derechos que tienen los trabajadores, al amparo de la *Ley Núm. 130*, para organizarse y ayudar a las organizaciones obreras a negociar colectivamente. Además, investiga y resuelve controversias de representación, para promover la negociación

colectiva con los representantes seleccionados por los trabajadores; determina de tiempo en tiempo las unidades apropiadas; investiga y resuelve casos de prácticas ilícitas del trabajo; y ayuda a poner en vigor los laudos de arbitrajes[1].

La Junta no tiene autoridad en la administración de la agencia, sólo constituye el cuerpo deliberativo y adjudicativo que emite decisiones finales en torno a las controversias que se le remiten de acuerdo con la *Ley Núm. 130*. Es responsable de implementar; en forma adecuada, eficaz e imparcial; la política pública gubernamental respecto a las relaciones obrero-patronales. Además, promueve los principios de la negociación colectiva al intervenir en disputas obrero-patronales en el ámbito sindical, con el fin de fomentar la paz industrial y la producción económica. La Junta tiene jurisdicción en los casos en que el patrono sea una corporación pública o un patrono privado que genere ingresos menos de $500,000 anuales y no esté involucrado en el comercio interestatal.

La Junta se rige por las opiniones del Tribunal Supremo de Puerto Rico, las reglas de evidencia de los tribunales y de procedimiento civil, y por la *Ley 38-2017, Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*[2]. Esta última establece el procedimiento a seguir para la solución de controversias administrativas de una agencia, de manera que se garantice que dicho procedimiento se efectúe de forma rápida y justa.

La Junta está compuesta por un presidente y dos miembros asociados nombrados por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico, por un término de 10 años. El presidente es el funcionario ejecutivo de la Junta. Las responsabilidades y funciones de la Junta son

---

[1] La Junta tiene la discreción para poner o no en vigor las decisiones emitidas por los organismos competentes en los casos de disputa obrero-patronal.

[2] Esta derogó la *Ley Núm. 170 del 12 de agosto de 1988, Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico*, según enmendada.

realizadas a través de sus distintas divisiones administrativas. Su cuerpo organizacional está integrado por la Oficina del Presidente y las divisiones de Secretaría, de Investigaciones, Legal, de Oficiales Examinadores y de Servicios Administrativos.

A la fecha de nuestra auditoría, la Junta tenía una infraestructura que constaba de 5 servidores, de los cuales 2 eran virtuales, 4 *switches*[3] y 27 computadoras, en las que se mantenía la información y las aplicaciones administrativas utilizadas por el personal. Además, contaba con una red de área local (*LAN*, por sus siglas en inglés) y una línea dedicada a Internet, que daba servicio a sus divisiones y oficinas ubicadas en los dos pisos del edificio. Los sistemas de información computadorizados eran administrados por el coordinador de sistemas de información, quien le respondía a la directora de la División de Servicios Administrativos.

Los recursos para financiar las actividades operacionales de la Junta provienen de la Resolución Conjunta del Presupuesto General y de Fondos Especiales Estatales. El presupuesto asignado, para los años fiscales del 2014-15 al 2016-17, ascendió a $1,503,000, $1,303,000 y $1,301,850[4], respectivamente.

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

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

---

[3] 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.

[4] El presupuesto asignado, para los años fiscales 2015-16 y 2016-17, fue ajustado por $25,000 y $150 para establecer una reserva presupuestaria bajo la custodia de la Oficina de Gerencia y Presupuesto, según establecido en las cartas circulares *124-15* y *133-16* del 7 de julio de 2015 y 17 de junio de 2016.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* y varias situaciones determinadas durante la auditoría, fueron remitidas al Lcdo. Jeffry J. Pérez Cabán, entonces presidente de la Junta, mediante carta de nuestros auditores del 20 diciembre de 2016. En la referida carta se incluyó un anejo con detalles sobre las situaciones comentadas.

El 18 de enero de 2017 el licenciado Pérez Cabán contestó la carta de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe* se remitió para comentarios, por cartas del 15 de noviembre de 2017, a la Lcda. Norma W. Méndez Silvagnoli, presidenta interina de la Junta. En el mismo se indicaron datos específicos, tales como los nombres de servidores, los cuales, por seguridad, no se incluyen en este *Informe*. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al licenciado Pérez Cabán, expresidente de la Junta.

El 5 de diciembre de 2017 la presidenta interina solicitó una prórroga para remitir sus comentarios, la cual le concedimos hasta el 8 de enero de 2018. Esta contestó el borrador mediante correo electrónico del 8 de enero. En los **hallazgos** se incluyeron algunos de sus comentarios.

Mediante correo electrónico del 21 de noviembre de 2017, el expresidente indicó, entre otras cosas, que se allanaba a los comentarios de la presidenta interina de la Junta.

CONTROL INTERNO

La gerencia de la Junta es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de este *Informe*. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno de la Junta.

En los **hallazgos** de este *Informe* se comentan las deficiencias de control interno significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado.

Además, mediante carta del 20 de diciembre de 2016 de nuestros auditores, le notificamos al entonces presidente sobre una deficiencia de control interno relacionada con la falta de auditorías sobre la seguridad, los procedimientos, los controles y las operaciones de los sistemas de información computadorizados de la Junta, la cual no es significativa para los objetivos de la auditoría.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la Junta, objeto de este *Informe*, se realizaron de acuerdo con las normas y la reglamentación aplicables, excepto por los **hallazgos del 1 al 5** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos, de un análisis de impacto de negocio de los sistemas de información computadorizados, y de un plan escrito 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 15 de septiembre de 2016, en la Junta 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 15 de septiembre de 2016, en la Junta no se había realizado un análisis de impacto de negocio sobre los sistemas de información computadorizados.

c. Al 15 de septiembre de 2016, la Junta no contaba con un plan o procedimiento 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 en los **apartados a. y c.** 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[5], aprobada el 8 de diciembre de 2004 por la directora de la Oficina de Gerencia y Presupuesto (OGP).

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-015, Programa de Continuidad Gubernamental*[6], 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 Junta estimar el impacto que los elementos de riesgos tendrían en las áreas y en 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 Junta, en caso de que surja alguna eventualidad.

La situación comentada en el **apartado c.** impide a la Junta 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 se atribuyen a que el presidente de la Junta desconocía que se debían preparar los análisis y el plan mencionados, ya que entendía que la OGP era quien se encargaba de regular y fiscalizar todo lo relacionado con los sistemas de información. Además, se debían a la falta de conocimiento especializado para preparar los mismos y a limitaciones presupuestarias.

---

[5] 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 Oficina de Gerencia y Presupuesto. Esta contiene disposiciones similares a las de la *Carta Circular* derogada.

[6] Dicha *Política* fue derogada por la *Carta Circular 140-16*, la cual contiene disposiciones similares.

Comentarios de la Gerencia

La presidenta interina nos indicó, entre otras cosas, lo siguiente:

> Durante los pasados meses, la Junta de Relaciones del Trabajo ha estado recopilando información necesaria para realizar informes de análisis de riesgos de los sistemas computadorizados de información y análisis de impacto de negocio o plan para el manejo de incidentes. Debido a la falta de conocimiento especializado y a limitaciones presupuestarias que dificultan la contratación externa para asistir en el proceso, la Junta no ha podido culminarlo. Además, los sistemas de tecnología de información de la Junta sufrieron daños, por lo cual tendrán que ser sustituidos. Toda vez que este hallazgo está relacionado al tipo de sistema que posee la agencia y que los que ésta posee actualmente van a ser sustituidos, la corrección de este hallazgo tendrá que ser aplazada. La Junta utilizará las herramientas y los recursos que se encuentren a su alcance y realizará todos los esfuerzos necesarios para lograr la corrección de este hallazgo en el menor tiempo posible. [*sic*]

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

Hallazgo 2 - Falta de un plan de continuidad de negocios, deficiencias relacionadas con el Plan de Contingencias, falta de pruebas o simulacros, y de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Al 4 de octubre de 2016, la Junta 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 los sistemas de información computadorizados y restaurar las operaciones de la Junta, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red de comunicación, o desastres naturales, entre otros.

b. La Junta contaba con el *Plan de Contingencias* (*Plan*) aprobado el 28 de diciembre de 2010 por el presidente. El mismo tenía el objetivo de establecer los procedimientos a seguir antes, durante y después de la declaración de un desastre.

El examen realizado el 29 de noviembre de 2016 al *Plan* reveló las siguientes deficiencias:

1) El *Plan* no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

   - El nombre del encargado de activar el *Plan*
   - Una lista detallada con todos los medios de comunicación de los diferentes miembros de cada grupo de recuperación, incluidos los empleados del área de sistema de información
   - El plan general de acción identificado por grupos y tareas de forma secuencial
   - El detalle de la configuración de los equipos críticos (equipos de comunicación y servidores) y del contenido de los respaldos y 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
   - Los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información de los usuarios que acceden a los sistemas de información de la Junta mediante conexiones remotas
   - Un itinerario de restauración que incluya el orden de las aplicaciones a recuperar y los procedimientos para restaurar los respaldos
   - Una lista de proveedores de servicios principales que incluya el número de teléfono y el nombre del personal de enlace con la entidad
   - La identificación de equipos de telecomunicaciones y computadoras compatibles con los de la Junta

- Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

2) El *Plan* no estaba actualizado. El mismo estaba fundamentado en la *Guía Núm. 6 - Plan de Contingencia*, de la *Carta Circular 96-01*, promulgada el 25 de septiembre de 1995 por el Comité del Gobernador, sobre sistemas de información, la cual estaba derogada desde el 15 de diciembre de 2004.

c. Al 14 de noviembre de 2016, la Junta no había realizado pruebas o simulacros que certificaran la efectividad del *Plan*.

d. No mantenía una copia del *Plan* ni de la documentación de los sistemas de información y de las aplicaciones, en un lugar seguro fuera de las instalaciones de la Junta.

e. Al 4 de septiembre de 2016, la Junta no contaba con un centro alterno de los sistemas de información para restaurar las operaciones críticas computadorizadas en casos de emergencia.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*[7].

Lo comentado en los **apartados del a. al c.** se aparta de lo establecido en la *Política TIG-015*[8].

La situación comentada en el **apartado c.** es contraria a lo establecido en el Capítulo II, Activación del Plan de Contingencia, Revisión de Procesos y Responsabilidades; Prueba anual de restauración de Datos del *Plan*.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan copia actualizada de los planes de contingencias y la documentación de las configuraciones de los sistemas, las aplicaciones y los programas críticos, en un lugar seguro

[7] Véase la nota al calce 5.

[8] Véase la nota al calce 6.

fuera del edificio donde ubica el centro. Esto es necesario para la pronta continuidad de las operaciones, en caso de que ocurra un evento inesperado. **[Apartado d.]**

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

- 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 del a. al d.** pueden propiciar la improvisación y que, en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios ofrecidos a los usuarios de la Junta.

La situación comentada en el **apartado e.** podría afectar las operaciones de la Junta, 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 Junta.

Causas

La situación comentada en el **apartado a.** se atribuye a la falta de un análisis de riesgos de los sistemas de información computadorizados de la Junta que sirva de base para la preparación y la revisión de un plan de continuidad de negocios que incluya un plan de contingencia con los requisitos necesarios para atender eventos o situaciones de emergencia. **[Véase el Hallazgo 1-a.]**

Las situaciones comentadas en los **apartados b., d. y e.** se debían, en parte, a que el presidente no había impartido instrucciones a la directora de la División de Servicios Administrativos para que actualizara el *Plan*; mantuviera copia de este, de la documentación de los sistemas y de las aplicaciones en un lugar seguro fuera de los predios de la Junta; y coordinara la identificación de un lugar disponible y adecuado como centro alterno para restaurar las operaciones computadorizadas críticas de la Junta.

La situación comentada en el **apartado c.** se debía, en parte, a que la directora de la División de Servicios Administrativos alegó que no contaban con la experiencia, la pericia, la destreza y los recursos adecuados para la realización de las pruebas o simulacros.

Comentarios de la Gerencia

La presidenta interina nos indicó, entre otras cosas, lo siguiente:

> La Junta de Relaciones del Trabajo ha estado recopilando información necesaria para preparar un plan de continuidad de negocios e identificar un centro alterno de recuperación de operaciones computadorizadas. Para ello, ha realizado acercamientos con dos agencias que pueden colaborar con este propósito. [...] **[Apartados a. y e.]**

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

Hallazgo 3 - Deficiencias relacionadas con los parámetros de seguridad configurados en el servidor principal, y falta de documentación de revisiones periódicas

Situaciones

a. Para llevar a cabo las operaciones y brindar sus servicios, la Junta contaba con cinco servidores, entre estos, el servidor principal para acceder a la red de comunicación y el que permitía el acceso a Internet a los usuarios autorizados. Los servicios de correo electrónico *Office 365* de la Junta eran provistos a través de la red interagencial mediante el contrato global de licenciamiento entre *Microsoft* y la OGP. A cada agencia se le creaba un dominio individual y la misma era responsable de la administración y creación de sus cuentas de acceso.

1) El examen efectuado el 20 de octubre de 2016, sobre los parámetros de seguridad definidos en el sistema operativo del servidor principal de la Junta, reveló que no estaban definidas:

   a) La política relacionada con las contraseñas de las cuentas de acceso para requerir que, las que fueran utilizadas, tuvieran combinaciones alfanuméricas (*Password must meet complexity requirements*).

   b) Las políticas de control de cuentas (*Account Lockout Policy*), para establecer lo siguiente:

      - Al menos, cinco intentos fallidos antes de desactivar la cuenta (*Account lockout threshold*)
      - El tiempo que debía permanecer la cuenta desactivada en casos de desactivarse la misma por intentos de acceso fallidos (*Account lockout duration*)
      - El tiempo de la instrucción para reiniciar el conteo de intentos para acceder a los recursos de la red sin éxito (*Reset account lockout counter after*).

   c) Las políticas de auditoría (*Audit Policy*) para que el sistema produjera un registro de los siguientes eventos:

      - La solicitud al servidor para validar las cuentas de usuario (*Audit account logon events*)
      - La creación, modificación o eliminación de una cuenta o grupo de usuarios; el cambio de nombre o contraseña; y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)
      - El acceso al directorio de servicio (*Audit directory service access*)
      - La activación y desactivación de las cuentas (*Audit logon events*)

- Los accesos a los archivos, fólders e impresoras (*Audit object access*)
- Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)
- El uso de los privilegios asignados a los usuarios (*Audit privilege use*)
- Las acciones ejecutadas por algún programa (*Audit process tracking*)
- El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*).

d) Las políticas sobre los privilegios asignados a los usuarios (*User Rights Assignment*).

e) Las opciones de seguridad (*Security Options*), excepto la opción de desactivar automáticamente del sistema al usuario, una vez venciera el término de acceso a los recursos de la red, previamente establecido (*Do not force logoff when logon hours expire)*, la cual no se había activado (*Disabled*).

2) Al 4 de octubre de 2016, el coordinador de sistemas de información no mantenía la documentación de las revisiones periódicas realizadas a los registros de seguridad producidos por el sistema operativo sobre el acceso a los sistemas de información computadorizados, y el uso de Internet y del correo electrónico. Esto, para evidenciar el examen de las violaciones de seguridad que pudieran ocurrir en el servidor y en la red, la auditoría de las páginas en Internet que acceden los usuarios autorizados y las transacciones del correo electrónico. Además, para registrar las medidas preventivas y correctivas tomadas.

Criterio

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*[9]. 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. También 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 lo siguiente:

- El uso de contraseñas complejas para acceder a los sistemas de información
- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos
- La activación de todas las opciones para registrar los eventos de seguridad de las aplicaciones y del sistema operativo
- La limitación del tiempo de acceso para todas las cuentas de acceso de acuerdo con las funciones de cada usuario
- La impresión y revisión periódica de las bitácoras (*logs*) que proveen cada herramienta, en las que se detallan los accesos de los usuarios a los sistemas de información computadorizados, la información accedida, las páginas en Internet visitadas y las transacciones de correo electrónico.

[9] Véase la nota al calce 5.

Efectos

Las situaciones comentadas en el **apartado a.1)a), y del c) al e)** pueden propiciar que personas no autorizadas accedan a información confidencial mantenida en los sistemas computadorizados y puedan hacer uso indebido de esta. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Lo comentado en el **apartado a.1)b)** impide a la Junta mantener un registro de los eventos inusuales o los problemas ocurridos en la red, que le permita al coordinador de sistemas de información tomar a tiempo las medidas correctivas o preventivas necesarias.

Lo comentado en el **apartado a.2)** privó a la gerencia de los medios necesarios para supervisar eficazmente el desempeño de los usuarios, y evidenciar los casos en que se detecte el acceso y uso indebido de los sistemas computadorizados, del Internet y del correo electrónico.

Causas

Las situaciones comentadas se debieron a que:

- La directora de la División de Servicios Administrativos de la Junta no veló por que el coordinador de sistemas de información pusiera en vigor todas las opciones de seguridad de acceso lógico que provee el sistema operativo del servidor principal. **[Apartado a.1)]** Además, no había impartido instrucciones a este para que documentara la revisión periódica de los registros de acceso a los sistemas de información computadorizados, a Internet y al correo electrónico. **[Apartado a.2)]**

- El coordinador de sistemas de información, al ser el único empleado del área de sistemas de información, realizaba todas las funciones relacionadas con los sistemas de información computadorizados de la Junta. Por esto, se le hacía difícil documentar la revisión periódica de los registros de seguridad del acceso a los sistemas de información, a Internet y al correo electrónico. **[Apartado a.2)]**

Comentarios de la Gerencia

La presidenta interina nos indicó, entre otras cosas, lo siguiente:

> La Junta de Relaciones del Trabajo ha impartido instrucciones al Coordinador de Sistemas de Información para subsanar las deficiencias relacionadas con los parámetros de seguridad configurados en el servidor principal y con la falta de documentación de las revisiones periódicas de los registros de seguridad. [...]

Véase la Recomendación 2.c.

Hallazgo 4 - Falta de procedimientos escritos para la disposición de la información sensitiva y de los programas

Situación

a. La Junta, entre otras cosas, atiende los casos relacionados con la *Ley 333-2004, Carta de Derechos de los Empleados de una Organización Laboral*, y los reclamos relacionados con la *Ley 66-2014*.

   La información relacionada con el formulario de radicación de querellas se registra en el Sistema de Casos. Este contiene información del trámite de las solicitudes recibidas en virtud de las leyes mencionadas. La información registrada en la aplicación incluye, entre otras cosas, el nombre, el número de teléfono, el correo electrónico; y la dirección residencial y postal de todas las personas involucradas en el caso. Además, incluye la información de los hechos o las controversias de cada caso. Como parte del trabajo relacionado con la resolución de los casos, los empleados asignados utilizan computadoras para redactar informes, interrogatorios, mociones para los tribunales, memorandos y laudos, entre otros. Dichos documentos los almacenan en un espacio designado a cada empleado en un servidor.

   Al 4 de octubre de 2016, en la Junta no se había promulgado un procedimiento para reglamentar y controlar eficazmente la disposición de la información sensitiva y de los programas mantenidos en los equipos y sistemas de información computadorizados, antes de transferir o disponer los mismos.

Criterios

La situación comentada es contraria a lo establecido en las políticas *TIG-003 y TIG-007, Disposición de Equipo y Licencias* de la *Carta Circular 77-05*[10].

Efectos

La situación comentada puede propiciar que, al momento de transferir o disponer de los equipos computadorizados, no se considere la eliminación de la información confidencial y de los programas almacenados en los mismos. Esto, a su vez, puede ocasionar que personas no autorizadas logren acceso a información confidencial mantenida en los sistemas computadorizados, y que la misma sea divulgada o utilizada indebidamente. También podría ocasionar situaciones que afecten los derechos de terceros, por las cuales se responsabilice a la Junta.

Causa

La situación comentada se atribuye a que el presidente de la Junta desconocía que debía promulgar la reglamentación mencionada.

Comentarios de la Gerencia

La presidenta interina nos indicó, entre otras cosas, lo siguiente:

> La Junta de Relaciones del Trabajo ha impartido instrucciones al Coordinador de Sistemas de Información para subsanar las deficiencias relacionadas con la disposición de información sensitiva y de los programas. Dicha instrucción fue notificada también a la Directora de la División de Servicios Administrativos. [...]

Véase la Recomendación 2.a.3).

Hallazgo 5 - Falta de un registro de los problemas relacionados con los equipos conectados a la red

Situación

a. Al 19 de octubre de 2016, la Junta no contaba con un registro de los problemas confrontados con los equipos conectados a la red,

[10] Véase la nota al calce 5.

sus causas y el tiempo transcurrido para resolverlos. Esto, para que, en caso de que se repitieran, pudiera hacerse referencia a la solución dada a los mismos.

Criterio

La situación comentada se aparta de lo establecido en la *Política TIG-004, Servicios de Tecnología*, de la *Carta Circular 77-05*[11]. En esta se establece que el personal de la oficina de tecnología de información de la agencia será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos. Además, revisará regularmente sus sistemas para verificar que funcionen adecuadamente. En consonancia con esto, para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados, se debe mantener un registro, en el cual se anoten los problemas surgidos con los equipos conectados a la red, sus causas, el tiempo transcurrido para resolverlos, y cómo estos fueron resueltos.

Efectos

La situación comentada priva al coordinador de sistemas de información de las herramientas y los mecanismos necesarios para identificar los problemas existentes relacionados con los equipos conectados a la red. Además, le impide a la Junta tener un control eficaz y documentado sobre el manejo de los problemas ocurridos con estos equipos, y que se puedan tomar las medidas para minimizar su efecto y prevenir su reincidencia, en caso de que el coordinador de sistemas de información no esté presente.

Causa

La situación comentada se debía a que el presidente de la Junta no había promulgado una directriz para que se preparara un procedimiento para el mantenimiento de los equipos conectados a la red, que requiera establecer un registro para documentar los problemas relacionados con estos.

---

[11] Véase la nota al calce 5.

Comentarios de la Gerencia

La presidenta interina nos indicó, entre otras cosas, lo siguiente:

> La Junta de Relaciones del Trabajo ha impartido instrucciones al Coordinador de Sistemas de Información para subsanar las deficiencias relacionadas con los equipos conectados a la red. Dicha instrucción fue notificada también a la Directora de la División de Servicios Administrativos. [...]

Véase la Recomendación 2.a.4).

RECOMENDACIONES

A la Presidenta Interina de la Junta de Relaciones del Trabajo de Puerto Rico

1. Asegurarse de que se realicen y documenten los análisis de riesgos de los sistemas de información computadorizados y de impacto de negocio, según se establece en las políticas *ATI-003, Seguridad de los Sistemas de Información,* y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*, y que los mismos sean remitidos para su revisión y aprobación. **[Hallazgo 1-a. y b.]**

2. Ejercer una supervisión efectiva sobre la directora de la División de Servicios Administrativos para asegurarse de que:

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

      1) Un procedimiento relacionado con el manejo de incidentes. Como parte de dicho procedimiento, se debe requerir que se documenten todos los incidentes y se indique cómo se resolvieron de manera que, cuando estos se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones. **[Hallazgo 1-c.]**

      2) Un 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 las políticas *ATI-003 y ATI-015*. 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 y de la documentación de los sistemas y de las aplicaciones en un lugar seguro fuera de lo predios de la Junta. **[Hallazgo 2-a., c. y d.]**

3) Las normas y los procedimientos necesarios para reglamentar el proceso de disposición de información sensitiva y de los programas, antes de transferir o dar de baja a los equipos computadorizados y los medios de almacenamiento de información, basados en lo establecido en la *Política ATI-007, Disposición de Equipo y Licencias de la Carta Circular 140-16*. **[Hallazgo 4]**

4) Un procedimiento para el mantenimiento de los equipos conectados a la red que requiera establecer un registro de los problemas relacionados con estos. **[Hallazgo 5]**

b. Enmiende el *Plan de Contingencias* para que incluya los aspectos comentados en el **Hallazgo 2-b.**, y lo remita para aprobación.

c. Imparta instrucciones al coordinador de sistemas de información para que:

1) Evalúe las opciones correspondientes a las políticas de las contraseñas de las cuentas de acceso (*Password Policy*) y 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 los sistemas de información de la Junta. **[Hallazgo 3-a.1)]**

2) Documente las revisiones realizadas a los registros de seguridad de acceso a los sistemas de información computadorizados, a Internet y al correo electrónico, y las medidas preventivas y correctivas tomadas durante el proceso. **[Hallazgo 3-a.2)]**

3. Realizar las gestiones necesarias para que la Junta cuente con un centro alterno para la recuperación de sus operaciones computadorizadas. **[Hallazgo 2-e.]**

APROBACIÓN

A los funcionarios y a los empleados de la Junta de Relaciones del Trabajo de Puerto Rico, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

ANEJO 1

JUNTA DE RELACIONES DEL TRABAJO DE PUERTO RICO
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

MIEMBROS PRINCIPALES DE LA JUNTA
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Jeffry J. Pérez Cabán	Presidente	31 may. 16	23 dic. 16
Lcdo. Edwin R. Viñas López	Miembro Asociado	31 may. 16	23 dic. 16
Vacante	"	31 may. 16	23 dic. 16

ANEJO 2

JUNTA DE RELACIONES DEL TRABAJO DE PUERTO RICO
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Jeffry J. Pérez Cabán	Presidente	31 may. 16	23 dic. 16
Sra. Yanira Barreto González	Directora de la División de Servicios Administrativos	31 may. 16	23 dic. 16
Sr. Israel Soto Vega	Coordinador de Sistemas de Información	31 may. 16	23 dic. 16

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr