INFORME DE AUDITORÍA TI-16-07

6 de mayo de 2016

Departamento de Corrección y Rehabilitación

Junta de Libertad Bajo Palabra

Oficina de Sistemas de Información

(Unidad 5351 - Auditoría 14026)

Período auditado: 21 de mayo al 30 de septiembre de 2015

CONTENIDO

Página

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

6 de mayo de 2016

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Junta de Libertad Bajo Palabra (Junta), adscrita al Departamento de Corrección y Rehabilitación (DCR), 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 21 de mayo al 30 de septiembre de 2015. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Junta se creó mediante la *Ley Núm. 118 del 22 de julio de 1974*, según enmendada. Su misión es decretar la libertad bajo palabra con discreción, independencia y juicio, de cualquier persona recluida en alguna de las instituciones penales de Puerto Rico, a los fines de mejorar la administración de la justicia en el País y lograr la integración del confinado a la libre comunidad.

La Junta es responsable de evaluar, conceder o revocar órdenes de arrestos y excarcelaciones, y hacer recomendaciones para clemencias ejecutivas al Gobernador, luego de un análisis ponderado de las mismas. Esto, con el fin de promover la rehabilitación del confinado, así como la seguridad de la comunidad. Para cumplir con su misión, la Junta ofrece sus servicios mediante los programas: Revisión de Casos de los Confinados para Determinación de Libertad Bajo Palabra, y Notificación a Víctimas.

Bajo el programa Revisión de Casos de los Confinados para Determinación de Libertad Bajo Palabra, se revisan los casos de los peticionarios referidos a la Junta, para otorgar o revocar el privilegio de libertad bajo palabra. Esto requiere que el peticionario cumpla con los requisitos y criterios dispuestos en ley y reglamento, y con un itinerario de horas de entrada y salida de su lugar de residencia, para disfrutar del privilegio. Como parte de este proceso y por delegación de los miembros de la Junta, los oficiales examinadores llevan a cabo vistas administrativas mediante un sistema interactivo de videoconferencia instalado en 11[1] programas de comunidad, 7[2] instituciones penales y en 5[3] salas de vistas. Durante los años fiscales del 2012-13 al 2014-15, el programa ofreció sus servicios a 21,871 confinados, concedió libertad bajo palabra a 904 confinados y denegó la libertad bajo palabra a 7,393 confinados.

[1] Localizados en Aguadilla, Aibonito, Arecibo, Bayamón, Caguas, Carolina, Guayama, Humacao, Mayagüez, Ponce y Utuado.

[2] Estas eran: Bayamón 1072, Guayama 500, Guayama 296, Guayama 1000, Campamento Zarzal, Jóvenes Adultos Ponce 304 y Ponce 1000.

[3] Estas se identifican con las letras de la A a la E.

A través del programa Notificación a Víctimas se les garantiza a las víctimas de todo delito el derecho de notificación, asistencia y participación en los procedimientos relacionados con la libertad bajo palabra de los convictos de delito. Esto, con el propósito de obtener una opinión informada de las víctimas del delito. Durante los años fiscales del 2012-13 al 2014-15, el programa citó a 12,657 víctimas de delito.

La Junta está compuesta por una presidenta, quien dirige la misma en sus funciones cuasijudiciales, y por cuatro[4] miembros asociados nombrados por el Gobernador, con el consejo y consentimiento del Senado. A la Presidenta le responde una directora ejecutiva, la cual está a cargo de los asuntos administrativos y operacionales de la Junta.

Para realizar sus funciones, la Junta cuenta con las oficinas de la Presidenta, de Secretaría, de Oficiales Examinadores y de Servicios Administrativos. Además, funcionalmente, la Junta mantiene una Oficina de Querellas, en la cual laboran nueve oficiales examinadores. A la Directora Ejecutiva le responden los directores de las oficinas de Presupuesto y Finanzas, Recursos Humanos, y Servicios Generales. El puesto de Director de Centro de Cómputos está vacante desde el 2006, por lo que el personal de la OSI le responde directamente a la Directora Ejecutiva. La OSI cuenta con un especialista de sistemas de información, un administrador de la red, un operador de entrada de datos y una auxiliar administrativo.

La infraestructura tecnológica de la Junta actualmente consiste de:

- Una red de área local para comunicar los servidores y las computadoras que se mantienen en uso. La conexión de la red se establece a través de 1 *router*[5] que pertenece a la Oficina de Gerencia y Presupuesto (OGP) y de 2 *switches*[6] que pertenecen al DCR. Además, la Junta utiliza 1 línea dedicada provista por la OGP para obtener acceso a Internet.

[4] Durante el período auditado, uno de los cuatro puestos de miembros asociados estuvo vacante.

[5] Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y tablas de direccionamiento.

[6] 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.

- Ocho servidores que están localizados en el Centro de Cómputos del Departamento de Educación (DE).
- Cuarenta y nueve computadoras y tres *laptops*.
- Veintitrés sistemas de videoconferencias, cuya conexión se establece a través de un modo de transferencia asíncrona (Red ATM)[7] del DCR.

Las transacciones financieras de la Junta se procesan a través del Puerto Rico Integrated Financial Accounting System (PRIFAS) del Departamento de Hacienda. Para el procesamiento de las transacciones de nómina y recursos humanos se utiliza el Sistema para el Registro de Asistencia (Kronos) y el Sistema de Recursos Humanos Mecanizados (RHUM) del Departamento de Hacienda.

Para cumplir con su misión, la Junta cuenta con cinco bases de datos que fueron desarrolladas internamente con el programa *Microsoft Access*. Estas son: Clemencias Ejecutivas, Casos Trabajados, Seguimiento de Casos, Mociones y Asesor Legal.

Los gastos operacionales de la OSI eran sufragados del presupuesto operacional de la Junta que, para los años fiscales del 2012-13 al 2014-15, fueron $2,325,000, $2,428,000 y $2,376,000, respectivamente.

El **ANEJO** contiene una relación de los 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.jlbp.gobierno.pr. 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* y otra situación determinada durante la auditoría, relacionada con la divulgación de información confidencial, fueron remitidas a la Lcda. Mercedes Peguero Moronta, Presidenta de la Junta, mediante carta de nuestros auditores, del 30 de septiembre de 2015. En la referida carta se incluyeron detalles sobre las situaciones comentadas.

[7] Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicaciones desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Mediante carta del 14 de octubre de 2015, la Presidenta remitió sus comentarios a dos de los hallazgos incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados al redactar el borrador de este *Informe*.

El borrador de 11 hallazgos se remitió para comentarios a la Presidenta de la Junta, y al Hon. Einar Ramos López, Secretario de Corrección y Rehabilitación, mediante cartas del 17 de marzo de 2016. El Secretario de Corrección y Rehabilitación, mediante carta del 12 de abril, indicó que había referido el borrador de los hallazgos a la Presidenta de la Junta y que le daría seguimiento a esta para que remita sus comentarios en el término establecido.

El 30 de marzo la Presidenta de la Junta solicitó prórroga para remitir sus comentarios y la misma fue concedida hasta el 15 de abril. Ese día recibimos su contestación en la cual indicó, entre otras cosas, lo siguiente:

> Deseamos informarle que estamos trabajando en cada uno de los hallazgos señalados en el borrador del informe. Aunque debido a la complejidad de alguno de ellos no hemos podido corregirlos en su totalidad, nos comprometemos a trabajar arduamente para cumplir con todas las exigencias de la Oficina del Contralor y la política pública del estado. [*sic*]

Luego de evaluar sus comentarios y la evidencia suministrada, determinamos que la Junta tomó las acciones correctivas pertinentes, excepto por los **hallazgos** de este *Informe*.

OPINIÓN Y HALLAZGOS

Opinión favorable con excepciones

Las pruebas efectuadas revelaron que las operaciones de la OSI, en lo que concierne a los controles internos establecidos para la administración de la seguridad, el acceso lógico y físico, la configuración de los sistemas de información, la continuidad del servicio, los controles para las computadoras y las aplicaciones, y la función de auditoría; se realizaron sustancialmente conforme a las normas generales aceptables en este campo, excepto por los **hallazgos del 1 al 7** que se comentan a continuación.

Hallazgo 1 - Deficiencia relacionada con la Evaluación de Riesgos de la Entidad

Situación

a. El análisis de riesgos de los sistemas de información computadorizados de una entidad es un proceso a través del cual se identifican los activos existentes de los mismos, 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.

   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.

   El 21 de mayo de 2015 se les suministró a nuestros auditores la *Evaluación de Riesgos de la Entidad*, aprobada el 10 de marzo de 2015 por la Presidenta de la Junta, como el informe de análisis de riesgo y de análisis de impacto de negocio. El examen realizado de la *Evaluación de Riesgos de la Entidad* reveló que la misma carecía de la identificación de todos los activos de sistemas de información (equipos, programas y datos) de la Junta. Por esto, en la *Evaluación* no se incluía la valoración y la clasificación de cada activo de acuerdo con la misión y los servicios de la Junta; la identificación de las vulnerabilidades y amenazas, y la probabilidad de ocurrencia de cada una de estas; ni el análisis de impacto de negocio correspondiente.

Criterios

La situación comentada es contraria 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*, aprobada el 8 de diciembre de 2004 por la Directora de la 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

La situación comentada impide a la Junta estimar el impacto que los elementos de riesgos tendrían sobre 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, dificulta 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.

Causa

La situación comentada se atribuye a que la Presidenta no había promulgado una directriz para que se tomara en consideración lo establecido en las políticas *TIG-003* y *TIG-015* durante la preparación, implementación y actualización continua de la *Evaluación de Riesgos de la Entidad*.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un plan de seguridad y de un procedimiento escrito para el manejo de incidentes

Situaciones

a. Al 21 de mayo de 2015, la Junta no tenía un plan de seguridad, aprobado por la Presidenta, que incluyera, entre otras cosas, disposiciones en cuanto a:

   - La documentación de la validación de las normas de seguridad[8]

[8] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el análisis de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

- La evidencia de un análisis de riesgo, que sea base del plan de seguridad
- La responsabilidad de la gerencia, del Administrador de la Red, del Especialista en Sistemas de Información, y de los demás componentes de la unidad
- Un programa de adiestramiento especializado al equipo clave de seguridad (Administrador de la Red y Especialista en Sistemas de Información)
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios, y que permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros)
- La documentación de la interconexión de los sistemas.

b. Al 10 de julio de 2015, la OSI 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.

Criterio

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Efectos

La situación comentada en el **apartado a.** podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

Lo comentado en el **apartado b.** le impide a la OSI 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.

Causa

Las situaciones comentadas se atribuyen a que la Presidenta de la Junta no había impartido directrices a la Directora Ejecutiva, quien supervisa las labores del personal de la OSI, para que esta requiera la preparación de un plan de seguridad, y el desarrollo y la aprobación de las normas y los procedimientos escritos para el manejo de incidentes.

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

Hallazgo 3 - Deficiencias relacionadas con el Plan de Contingencia del Centro de Cómputos de la Oficina de Sistemas de Información y Videoconferencia de la Junta de Libertad Bajo Palabra

Situaciones

a. El 14 de octubre de 2010 la Presidenta de la Junta aprobó el *Plan de Contingencia del Centro de Cómputos de la Oficina de Sistemas de Información y Videoconferencia de la Junta de Libertad Bajo Palabra* (*Plan*). Esto, con el propósito primordial de formalizar los procesos de recuperación de las operaciones computadorizadas que están relacionadas con los confinados y las víctimas de delito, en casos de situaciones de emergencia. Además, el documento tenía como fin prevenir una interrupción prolongada de los servicios, el incumplimiento de los tribunales o la pérdida de credibilidad ante las víctimas de delito y la ciudadanía en general.

   El examen efectuado al *Plan* reveló las siguientes deficiencias:

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

      - El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones
      - El detalle de toda la configuración de los equipos críticos (equipo de comunicación y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
      - El detalle de toda la configuración de los sistemas utilizados y requeridos para efectuar una restauración en un centro de cómputos 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.

2) El *Plan* no estaba actualizado. En el mismo se incluían los servidores *Exchange Server 2003, ISA Server 2004, File Server*, *Polycom Server, JLBPINTRANET, JLBP-WEB* y *Acuerdos* que la Junta no utilizaba. Además, en la Lista del Personal Clave del *Plan* se incluían los nombres de dos exfuncionarias, un exempleado, y del Especialista en Sistemas de Información como Director del Centro de Cómputos, puesto para el cual cesó funciones en diciembre de 2006. También el diagrama de la red no incluía representación de todos los servidores en uso, y el plan de desalojo no correspondía al piso donde está actualmente localizada la Junta.

3) De los procesos descritos en el *Plan* que continuaban en uso, no se efectuaban pruebas para asegurarse de la utilidad de los mismos.

b. En el *Plan* se indica que, entre los objetivos del plan de contingencia está identificar posibles lugares alternos donde se pueda reanudar el procesamiento de datos, de surgir algún desastre, y especificar los pasos necesarios para relocalizar el centro de operaciones en el lugar alterno. Sin embargo, al 15 de julio de 2015, la Junta no contaba con un lugar alterno para restaurar las operaciones computadorizadas en caso de emergencia. Tampoco había formalizado un acuerdo escrito con otra entidad para utilizar la instalación de esta como centro alterno.

Criterios

Las mejores prácticas en el campo de la tecnología de información, utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad

de los sistemas de información computadorizados, sugieren que, como parte del plan de continuidad de negocios, se prepare un plan de contingencias. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afecten su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la agencia 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. Además, se deben efectuar procedimientos para realizar pruebas o simulacros, por lo menos, una vez al año. **[Apartado a.]**

Estas prácticas también 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. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes: **[Apartado b.]**

- 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 el **apartado a.** 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 y de interrupciones prolongadas de los servicios ofrecidos a los usuarios de la Junta.

La situación comentada en el **apartado b.** podría afectar las funciones de la Junta y los servicios de la OSI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Eso podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la OSI.

Causas

Las situaciones comentadas se atribuyen a que la Presidenta no había promulgado una directriz para que la Directora Ejecutiva se asegure de que el *Plan* de la Junta incluya medidas de seguridad adecuadas, y el mismo se mantenga actualizado. **[Apartado a.]** Tampoco le había requerido a esta realizar las gestiones necesarias para identificar un lugar alterno y adecuado en el cual la Junta pueda restaurar las operaciones críticas computadorizadas, en caso de una emergencia. **[Apartado b.]**

Véanse las recomendaciones 1, y 4.b. y c.

Hallazgo 4 - Falta de diccionarios de datos y manuales de usuarios como documentación de las bases de datos desarrolladas internamente en la Junta

Situación

a. La Junta contaba con cinco bases de datos desarrolladas internamente por el Especialista en Sistemas de Información. Estas son:

- Seguimiento de Casos - Procesa los procedimientos relacionados con la población penal que ha sido convicta y sentenciada por un tribunal en Puerto Rico, y que ha sido referida por el DCR a la Junta para conceder o denegar la libertad bajo palabra. En esta también se mantiene información sobre las víctimas, las citaciones, los informes, entre otros.
- Casos Trabajados - Documenta todas las resoluciones emitidas por la Junta.
- Asesor Legal - Procesa todos los casos que refiere la Junta al Departamento de Justicia para procesamiento judicial.
- Clemencias Ejecutivas - Documenta la información relacionada con los convictos que solicitan el indulto del Gobernador o la conmutación de penas o multas, entre otros.
- Mociones - Procesa todas las mociones presentadas por la población penal, así como la solicitud de representación legal de los confinados.

El examen realizado el 3 de septiembre de 2015 relacionado con la documentación de estas bases de datos reveló que la Junta no contaba con un diccionario de datos[9] ni con un manual del usuario para cada una de estas. Esto, para proporcionar una comprensión clara y confiable de las bases de datos y, facilitar el mantenimiento y las modificaciones requeridas posteriormente.

Criterios

La situación comentada es contraria a lo establecido en la *Política TIG-011, Mejores Prácticas de la Infraestructura Tecnológica*, de la *Carta Circular 77-05*. En esta se indica que toda aplicación implementada deberá ser documentada mediante metodologías de documentación estándares o de uso común. Esta *Política* se establece, en parte, mediante el desarrollo y la actualización de la documentación de los sistemas.

Las normas generalmente aceptadas en el campo de la tecnología de información sugieren que las entidades deben mantener una documentación completa y actualizada de los sistemas en producción. Una documentación adecuada del funcionamiento de un sistema computadorizado y sus programas provee información esencial para la implementación y la operación eficaz de este. Esta es de utilidad para el desarrollo de programas complementarios y es fuente de información para el estudio y la evaluación de los controles internos y para el adiestramiento del personal nuevo.

Efectos

La situación comentada podría ocasionar dificultades a los usuarios para entender los procedimientos a seguir en el uso de las bases de datos. Además, podría dificultar la evaluación de controles y el adiestramiento del personal nuevo, en caso de ausencia prolongada del personal que efectuó el desarrollo interno.

[9] Base de datos que contiene el nombre, el tipo, el rango de valores, la fuente y la autorización para el acceso a cada elemento de los datos. Cuando la estructura de datos es considerada, también indica cuáles programas de la aplicación utilizan esos datos, de manera que se genere una lista de los programas afectados.

Causa

La situación comentada se atribuye a que la Directora Ejecutiva, como medida de seguridad, no había requerido mantener documentación de las bases de datos desarrolladas internamente.

Véanse las recomendaciones 1 y 4.d.1).

Hallazgo 5 - Deficiencias relacionadas con los parámetros de seguridad configurados en el sistema operativo del servidor principal de la red de la Junta

Situación

a. La OSI contaba con un servidor configurado como *Primary Domain Controller*, mediante el cual se controlaba el acceso a los recursos de la red de la Junta. El examen efectuado el 22 de julio de 2015 sobre los parámetros de seguridad establecidos en el sistema operativo de este servidor reveló que no estaban definidas:

    1) Las políticas relacionadas con las contraseñas de las cuentas de acceso (*Account Password Policy*) para requerir a los usuarios que utilizaran, al menos, cinco contraseñas diferentes antes de repetir una utilizada anteriormente (*Enforce Password History*).

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

        - Las solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*)
        - Los accesos de las cuentas (*Audit logon events*)
        - Los accesos a los archivos, los cartapacios (*folders*) y las impresoras (*Audit object access*)
        - El uso de los privilegios asignados a los usuarios (*Audit privilege use*)
        - Las acciones ejecutadas por algún programa (*Audit process traking*).

    3) Las políticas del registro de eventos en el sistema (*Events Logs*).

Criterio

La situación comentada 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 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:

- La configuración adecuada de 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.

Efectos

La situación comentada puede 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.

Causa

La situación comentada se debió a que la Directora Ejecutiva no veló por que el Administrador de la Red pusiera en vigor todas las opciones de seguridad de acceso lógico que provee el sistema operativo del servidor principal.

Véanse las recomendaciones 1 y 4.a.2).

Hallazgo 6 - Falta de toma de inventario de equipo computadorizado y de un registro de programas instalados en cada computadora

Situaciones

a. El Especialista en Sistemas de Información de la OSI es responsable, entre otras cosas, de mantener el inventario de propiedad de la Junta. El examen relacionado con la toma de inventario de los equipos y programas computadorizados de la Junta, reveló las siguientes deficiencias:

   1) Al 25 de junio de 2015, el Especialista no había realizado una toma de inventario desde el 2013. La toma del mismo se informó al Departamento de Hacienda el 29 de agosto de 2013. A mayo de 2015, la propiedad relacionada con tecnología de información

consistía de 152 activos adquiridos por $182,120. Entre estos, los 23 sistemas de videoconferencias utilizados para celebrar las vistas a los confinados.

2) Al 6 de julio de 2015, la OSI no mantenía un registro de los programas adquiridos e instalados en cada computadora que incluyera, entre otras cosas, lo siguiente:

- El número de licencia de los programas instalados
- El nombre del usuario
- El número de propiedad y la descripción de la computadora donde estaban instalados los programas
- El costo de los programas instalados.

Criterios

La situación comentada en el **apartado a.1)** es contraria a lo establecido en el Artículo 10(a) de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, y del Artículo XIV-A y D del *Reglamento 11, Normas Básicas para el Control y la Contabilidad de los Activos Fijos*, según enmendado, aprobado el 29 de diciembre de 2005 por el Secretario de Hacienda.

La situación comentada en el **apartado a.2)** es contraria a lo establecido en la *Política TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la *Carta Circular 77-05*. En esta se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas entidades gubernamentales.

Las mejores prácticas de la tecnología de información sugieren que se mantenga un registro de todos los programas, en el cual se indique lo siguiente: el número de la licencia, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el equipo donde está instalado (número de propiedad o de serie), la ubicación física de la licencia y de sus manuales, el nombre del usuario, el número de propiedad asignado, y el costo.

Efectos

Las situaciones comentadas le impiden a la Junta mantener un control efectivo sobre el equipo, la propiedad, los programas y las licencias correspondientes. Además, propician el ambiente para el uso indebido o la desaparición de la propiedad, y la instalación y el uso de programas no autorizados, sin que se puedan detectar estas situaciones a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la Junta. También dificulta nuestra gestión fiscalizadora, y el control que debe ejercer sobre la propiedad el Departamento de Hacienda.

Causa

Las situaciones comentadas se atribuyen a que la Directora Ejecutiva no se aseguró de que el Especialista en Sistema de Información, a cargo de la propiedad de la Junta, cumpliera con su responsabilidad de tomar y mantener un registro de inventario completo y actualizado del equipo y los programas computadorizados de la Junta.

Véanse las recomendaciones 1, y 4.d.2) y 3).

Hallazgo 7 - Falta de un proceso formal para el mantenimiento preventivo de los equipos conectados a la red y para documentar el apoyo técnico prestado a los usuarios de los sistemas de información computadorizados de la Junta

Situaciones

a. La Junta, como parte de su infraestructura tecnológica, posee una red de área local compuesta por 8 servidores, 49 computadoras y 3 *laptops*. Esto para, entre otras cosas, procesar y almacenar datos relacionados con las determinaciones y los acuerdos tomados sobre los confinados que solicitan libertad bajo palabra, e información de las víctimas.

   Al 15 de julio de 2015, la OSI no efectuaba un mantenimiento preventivo de los equipos principales conectados a la red, conforme a un itinerario o mecanismo formal. En su lugar, se ofrecía mantenimiento al equipo cuando confrontaba problemas o desperfectos.

b. Al 3 de septiembre de 2015, el personal de la OSI no utilizaba el sistema *Apoyo a Usuarios* desarrollado internamente por el Especialista en Sistemas de Información. Este sistema tenía como

propósito documentar los servicios de apoyo técnico que ofrecía el personal de la OSI a los usuarios de los sistemas de información computadorizados de la Junta. En su lugar, las solicitudes de apoyo técnico se generaban y atendían a través de comunicaciones telefónicas y correos electrónicos que no se documentaban.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-004, Servicios de Tecnología,* de la *Carta Circular 77-05.* 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.

Además, 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 agencias deberán desarrollar e implementar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente. Además, deberán desarrollar procedimientos para reportar y responder a incidentes. 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 incidentes con los sistemas de información y cómo estos fueron resueltos.

Efectos

La situación comentada en el **apartado a.** podría propiciar que las fallas en los equipos conectados a la red no sean detectadas a tiempo. Esto, a su vez, puede resultar en una falla mayor en la que se interrumpan las operaciones de la Junta y, por ende, los servicios que esta presta a sus usuarios.

La situación comentada en el **apartado b.** le impide a la OSI tener un control eficaz y documentado sobre el manejo del apoyo técnico ofrecido, con el objetivo de que se puedan tomar las medidas para minimizar los efectos de cualquier incidente y prevenir su reincidencia.

Causas

La situación comentada en el **apartado a.** se debió a que la Directora Ejecutiva no había impartido instrucciones al personal de la OSI para que implementara, como medida de control, un plan de mantenimiento preventivo de los equipos. Tampoco había requerido el uso del sistema *Apoyo a Usuarios* como mecanismo formal para identificar y documentar el apoyo técnico ofrecido a los usuarios. **[Apartado b.]**

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

RECOMENDACIONES

Al Secretario de Corrección y Rehabilitación

1. Ver que la Presidenta de la Junta cumpla con las **recomendaciones de la 2 a la 4** de este *Informe*. **[Hallazgos del 1 al 7]**

A la Presidenta de la Junta

2. Ver que se revise la *Evaluación de Riesgos de la Entidad* existente en la Junta para que se consideren e incluyan en el mismo los aspectos de análisis de riesgo y de impacto de negocio indicados en el **Hallazgo 1**, según se establece en las políticas *TIG-003* y *TIG-015*.

3. Realizar las gestiones necesarias para que la Junta cuente con un plan de seguridad para los sistemas de información, que incluya los criterios descritos en el **Hallazgo 2-a.** Una vez preparado, el mismo debe ser remitido para su revisión y aprobación. Además, ver que el mismo se divulgue a los funcionarios y empleados, y que se realicen evaluaciones periódicas para asegurar su funcionamiento.

4. Ejercer una supervisión efectiva sobre la Directora Ejecutiva que supervisa las labores de la OSI para asegurarse de que:

    a. El Administrador de la Red de la Junta realice las gestiones necesarias para:

        1) Preparar 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 2-b.]**

2) Configurar las opciones de seguridad de acceso lógico, que provee el sistema operativo del servidor, relacionadas con los aspectos comentados en el **Hallazgo 5**.

3) Establecer un itinerario formal para que se provea el servicio de mantenimiento preventivo requerido para los equipos computadorizados de acuerdo con las especificaciones de los manufactureros. **[Hallazgo 7-a.]**

b. El *Plan* incluya los detalles mencionados en el **Hallazgo 3-a.** Una vez actualizado, el mismo debe ser remitido para aprobación. Además, ver que se realicen evaluaciones y pruebas periódicas del mismo para asegurar su efectividad y funcionamiento.

c. Realice las gestiones necesarias para que se formalice un acuerdo escrito con un lugar alterno para la recuperación de las operaciones de la Junta, y el mismo incluya los términos y las condiciones, bajo los cuales este se utilizaría. **[Hallazgo 3-b.]**

d. El Especialista en Sistemas de Información realice las gestiones necesarias para:

1) Preparar los diccionarios de datos y los manuales de usuarios de las cinco bases de datos descritas en el **Hallazgo 4**, y provea copia del manual a los usuarios correspondientes.

2) Cumplir con lo establecido en la *Ley Núm. 230* y el *Reglamento 11* relacionado con el control y el manejo de los equipos de computadoras. **[Hallazgo 6-a.1)]**

3) Mantener un registro de los programas adquiridos por la Junta e instalados en las computadoras de esta que contenga, entre otra información, el número de la licencia y el costo de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde

están instalados los mismos. Esto, con el fin de mantener un inventario de los mismos y detectar la instalación de programas no autorizados. **[Hallazgo 6-a.2)]**

e. Requiera que el personal de la OSI utilice el sistema *Apoyo a Usuarios*, o uno similar, como mecanismo formal para identificar y documentar el apoyo técnico ofrecido a los usuarios. **[Hallazgo 7-b.]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yasmin M Valdivieso

ANEJO

DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN
JUNTA DE LIBERTAD BAJO PALABRA
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. José A. Aponte Carro	Secretario de Corrección y Rehabilitación Interino	21 may. 15	30 sep. 15
Lcda. Mercedes Peguero Moronta	Presidenta de la Junta	21 may. 15	30 sep. 15
Lcda. Carla M. Rodríguez Heredia	Miembro Asociado	21 may. 15	30 sep. 15
Sra. Silkia Figueroa Sierra	"	21 may. 15	30 sep. 15
Sra. Ana M. Silva Torres	"	21 may. 15	30 sep. 15
Vacante	"	21 may. 15	30 sep. 15
Sra. Marie J. Díaz Valcárcel	Secretaria de la Junta	21 may. 15	30 sep. 15
Lcda. Yailette De Jesús Cruz	Directora Ejecutiva	21 may. 15	30 sep. 15

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