Informe de Auditoría

TI-18-14

INFORME DE AUDITORÍA TI-18-14

11 de junio de 2018

Departamento de Justicia

Sistema de Información de Justicia Criminal

(Unidad 5275 - Auditoría 14092)

Período auditado: 25 de enero de 2016 al 15 de junio de 2017

CONTENIDO

Página

OBJETIVOS DE AUDITORÍA **2**

CONTENIDO DEL INFORME **2**

ALCANCE Y METODOLOGÍA **3**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **6**

CONTROL INTERNO **8**

OPINIÓN Y HALLAZGOS **9**

1 - Falta del Protocolo para Garantizar la Comunicación Efectiva entre los Componentes de Seguridad del Estado Libre Asociado de Puerto Rico, y de un plan de trabajo aprobado por el Comité 9

2 - Atraso en la validación de los registros migrados al RCI 11

3 - Falta de un plan de continuidad de negocios, un plan de contingencias sobre los sistemas de información, un centro alterno para la recuperación de las operaciones computadorizadas, y copias de respaldo fuera de las instalaciones del SIJC 15

4 - Incidente relacionado con el acondicionador de aire del Centro de Datos, que puso en riesgo la continuidad de las operaciones del SIJC 18

5 - Accesos al SORNA otorgados a empleados del DCR que no lo utilizaban, y falta de revisiones de las transacciones realizadas por sus usuarios y los del RCI 22

6 - Falta de una metodología formal para la adquisición y el desarrollo de aplicaciones 25

RECOMENDACIONES **26**

APROBACIÓN **29**

ANEJO 1 - MIEMBROS PRINCIPALES DEL COMITÉ INTERGUBERNAMENTAL DURANTE EL PERÍODO AUDITADO **30**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **31**

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

11 de junio 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 del Sistema de Información de Justicia Criminal (SIJC) del Departamento de Justicia (Departamento). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVOS DE AUDITORÍA

Determinar si las operaciones del SIJC; en lo que concierne a los controles internos para la administración de la seguridad, el acceso lógico y físico, la continuidad del servicio, la segregación de deberes, los equipos computadorizados, y la entrada de datos en el *Registro Criminal Integrado* (RCI) y en el *Registro de Personas Convictas por Delitos Sexuales y Abuso contra Menores* (SORNA); se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos. Además, determinar si las operaciones del SIJC, en lo que concierne a la contratación de servicios profesionales para el desarrollo del RCI, se realizaron conforme a las normas aplicables para el desarrollo de aplicaciones.

CONTENIDO DEL INFORME

Este *Informe* contiene seis hallazgos del resultado del examen que realizamos de lo indicado en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 25 de enero de 2016 al 15 de junio de 2017. En algunos aspectos examinamos operaciones 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 empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad 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

El SIJC está adscrito al Departamento de Justicia y su función es recibir, custodiar y proveer información de naturaleza penal. Mediante la *Ley 143-2014, Ley del Protocolo para Garantizar la Comunicación Efectiva entre los Componentes de Seguridad del Estado Libre Asociado de Puerto Rico y del Sistema de Información de Justicia Criminal*[1], se crea el Comité Intergubernamental (Comité) para dirigir el SIJC, y se designan sus funciones y responsabilidades. A la fecha de nuestra auditoría, el Comité estaba integrado por el secretario de Justicia, quien lo presidía, el director administrativo de los tribunales, el superintendente de la Policía, el secretario de Corrección y Rehabilitación, el secretario de Transportación y Obras Públicas, el secretario de la Familia y el director ejecutivo del Instituto de Ciencias Forenses, o las personas con funciones

[1] La *Ley 143-2014* derogó la *Ley 129* del 30 de junio de 1977 que estableció inicialmente el SIJC con el fin de proveer, de forma rápida, correcta e ininterrumpida, información de las personas convictas, los eventos de procedimiento criminal y las disposiciones que resulten de estos, tales como: arresto, radicación de acusación, sentencia y reclusión.

similares que estos designen. El SIJC debe proveer a los miembros del Comité información de naturaleza penal completa, actualizada y correcta. Entre las funciones y responsabilidades del Comité, está la designación del director administrativo del SIJC y la delegación de sus funciones.

Por disposición de la *Ley 266-2004, Ley del Registro de Personas Convictas por Delitos Sexuales y Abuso contra Menores*, según enmendada, el SIJC también es responsable de crear y mantener la operación del SORNA. Esto, con el propósito de proteger a la comunidad contra actos constitutivos de abuso sexual y abuso contra menores. Además, por disposición de la *Ley 300-1999, Ley de Verificación de Historial Delictivo de Proveedores de Servicios de Cuidado a Niños y Envejecientes*[2], según enmendada, es responsable de adoptar, promover e implementar mecanismos de prevención para el maltrato y abuso físico o sexual contra niños y envejecientes en las instalaciones de cuidado.

A la fecha de nuestra auditoría, la estructura organizacional del SIJC estaba compuesta por las oficinas del director administrativo y de Operaciones y Control, y por la Unidad de Análisis de Sistema. El SIJC contaba con 1 director administrativo, 1 subdirectora administrativa, 1 director de análisis y programación de sistemas de información, 1 supervisor de operaciones de procesamiento de datos, 1 analista estadístico, 1 coordinadora de entrada de datos, 2 técnicos de procesamiento de datos, 1 técnico de telecomunicaciones, 2 especialistas de validación de récords y 1 oficial legal. Además, contaba con 17 oficinistas de entrada de datos, 2 coordinadores de entrada de datos y 1 técnico de control de calidad y documentos, que laboraban en las

[2] Conforme con esta *Ley*, los proveedores de servicios de cuidado a niños y envejecientes deben contar con una certificación, expedida por la Policía de Puerto Rico, de que no aparecen registrados en el SORNA y el RCI.

fiscalías de distrito[3], y 5 empleados que laboraban en destaque en la Policía de Puerto Rico, la Oficina del Procurador de Menores, la Oficina del Jefe de los Fiscales y la División de Integridad Pública y Asuntos del Contralor. El SIJC tenía 85 puestos vacantes y contaba con los servicios contratados de 2 especialistas de validación de récords.

La infraestructura tecnológica del SIJC estaba compuesta por una red de área amplia (*WAN*, por sus siglas en inglés)[4] a la que se conectaban 60 agencias locales y federales. Además, contaba con una plataforma de nube privada[5]. La misma se compone de 16 servidores físicos[6] y 80 servidores virtuales[7] en los que manejaban las siguientes aplicaciones principales:

- RCI - Mantiene la información del proceso judicial de un ciudadano acusado, desde el registro de la querella de la Policía hasta la sentencia o determinación emitida por el tribunal. Sustituyó el *Registro Criminal Centralizado* (RCC) y su información se utiliza desde el 2013 para producir los certificados de antecedentes penales emitidos por la Policía; y para realizar investigaciones sobre individuos imputados de delitos y determinar reincidencias, entre otras cosas.
- SORNA - Mantiene la información registrada por la Policía de los adultos convictos por delitos sexuales y abuso contra menores. Incluye un módulo que, desde el 2014, permite acceso a los ciudadanos para verificar la información de los ofensores y su área de residencia.

---

[3] Las fiscalías de distrito son unidades de la Oficina del Jefe de los Fiscales a cargo de realizar investigaciones y procesar los casos de naturaleza penal en la jurisdicción del Estado Libre Asociado de Puerto Rico. También gestionan asuntos de naturaleza civil o administrativa, necesarios para imponer responsabilidad a los sujetos de la investigación o del proceso penal, e insta acciones para la restitución de fondos y propiedad obtenida de la comisión de delitos de corrupción gubernamental, crimen organizado y sustancias controladas.

[4] Red de computadoras que une varias redes locales, aunque todos sus miembros no estén en una misma ubicación física.

[5] Se refiere al uso de la tecnología de informática en la nube (*cloud computing*), en la que solamente una organización tiene acceso a los recursos que se utilizan para implementarla. La tecnología de informática en la nube permite ofrecer servicios a través de una red, que usualmente es Internet.

[6] Computadora destinada a almacenar, administrar, procesar y proveer información a otras computadoras en la red.

[7] Partición dentro de un servidor físico que habilita varias computadoras virtuales por medio de varias tecnologías.

El SIJC contaba con otros tres servidores físicos para mantener el *Automated Fingerscan Information System* (AFIS), que pertenecía a la Policía, y era utilizado para recopilar la información de las huellas digitales; y la plataforma y el servicio requerido para acceder e intercambiar, de forma segura, las transacciones con los sistemas del *Federal Bureau of Investigation* (FBI), entre estos, el *National Crime Information Center* (NCIC)[8] y la *National Law Enforcement Telecommunication System* (NLETS)[9].

El presupuesto asignado al SIJC provenía de las resoluciones conjuntas del presupuesto general, asignadas a través del Departamento, y de fondos federales. El presupuesto asignado para los años fiscales del 2014-15 al 2016-17 ascendió a $3,206,000, $3,162,148 y $2,853,000, respectivamente.

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

El SIJC cuenta con una página en Internet a la cual se puede acceder mediante la siguiente dirección: www.sijc.pr.gov. Esta página ofrece información acerca de los servicios que ofrece esta entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos 1, 3 y 4** de este *Informe* y otras situaciones determinadas durante la auditoría, fueron remitidas al Lcdo. César R. Miranda Rodríguez, entonces secretario de Justicia, mediante carta del 16 de noviembre de 2016. Además, las situaciones comentadas en los **hallazgos 2, 5 y 6**, y otras situaciones determinadas

[8] Es la base de datos central de los Estados Unidos, en la cual se mantiene información de naturaleza criminal. Es administrada a través de la *Criminal Justice Information Services* (CJIS) *Division* del FBI, y a la cual acceden agencias locales, estatales y federales.

[9] Red interestatal para el intercambio de información relacionada con el cumplimiento de ley, la justicia criminal y la seguridad pública entre los Estados Unidos, sus jurisdicciones y territorios. A través de la NLETS, el SIJC realiza envíos automáticos de información criminal mantenida en el RCI, que es utilizada por el *National Instant Criminal Background Check System* (*NICS*), para realizar la verificación al instante de antecedentes criminales, y permite a los concesionarios de ventas de armas y explosivos verificar si los prospectos compradores son elegibles para adquirirlas, según requerido por la *Brady Handgun Violence Prevention Act of 1993*. El sistema está diseñado para responder dentro de 30 minutos las consultas de verificación de antecedentes.

durante la auditoría, fueron remitidas a la Hon. Wanda Vázquez Garced, secretaria de Justicia, mediante cartas del 15 y 27 de junio de 2017. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

El 16 de diciembre de 2016 y el 10 de julio de 2017, el entonces secretario y la secretaria, contestaron las cartas de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe*, que incluía 8 hallazgos, se remitió a la secretaria de Justicia, para comentarios, por carta del 25 de abril de 2018. En este se indicaron datos específicos, tales como: nombres de las cuentas de acceso, los usuarios, los servidores y las compañías contratadas, y números de facturas y de sentencias por delitos graves y menos graves. Con el mismo propósito, remitimos el borrador de 8 hallazgos al licenciado Miranda Rodríguez, y de 1 hallazgo a los licenciados Luis Sánchez Betances y Guillermo Somoza Colombani, exsecretarios, mediante cartas de esa misma fecha.

El 17 de mayo la secretaria contestó y, luego de evaluar sus comentarios, determinamos no incluir en este *Informe* dos de los hallazgos remitidos. En los **hallazgos** incluidos se consideraron algunos de sus comentarios.

El licenciado Miranda Rodríguez contestó el borrador de los hallazgos mediante carta del 11 de mayo. En su contestación indicó, entre otras cosas lo siguiente:

> [...] Efectivamente algunos procesos en vías de implantación no se lograron completar al objetivo deseado ante la falta de recurso económico adecuado. Pero aun en esos casos, siempre se adoptaron medidas que propiciaran la continuidad y ocasionara el mejoramiento de los servicios en tales proyectos. [*sic*]
>
> [...] Muchas operaciones del RCI se lograron salvar pese a las limitaciones económicas que la situación fiscal del País nos impuso, y continúan imponiendo, cual bien se reconoce en el informe de hallazgos. [*sic*]

> [...] es necesario el que se continúe trabajando diligentemente para salvar cualquier incumplimiento identificado por su Oficina, conforme el informe de hallazgos presentado.

Los licenciados Sánchez Betances y Somoza Colombani no contestaron.

CONTROL INTERNO

La gerencia del SIJC 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 el objetivo de este *Informe*. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno del SIJC.

En los **hallazgos del 2 al 6** de este *Informe* se comentan las deficiencias de controles internos significativas, dentro del contexto del objetivo de nuestra auditoría, identificadas a base del trabajo realizado. Además, en el **Hallazgo 1** se comenta una deficiencia de control interno, relacionada con la falta del *Protocolo para Garantizar la Comunicación Efectiva entre los Componentes de Seguridad del Estado Libre Asociado de Puerto Rico*, y de un plan de trabajo aprobado por el Comité, la cual no es significativa para el objetivo de la auditoría, pero merece que se tomen medidas correctivas.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que podrían 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 el objetivo de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones del SIJC, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

Hallazgo 1 - Falta del Protocolo para Garantizar la Comunicación Efectiva entre los Componentes de Seguridad del Estado Libre Asociado de Puerto Rico, y de un plan de trabajo aprobado por el Comité

Situaciones

a. Mediante la *Ley 143-2014*, se asignó al Comité la responsabilidad de dirigir el SIJC. También se le asignaron los deberes y las funciones que debía realizar, entre estos, aprobar por mayoría simple los acuerdos del Comité y establecer y promulgar las reglas y reglamentos para el SIJC, de acuerdo al ordenamiento legal vigente. Además, mediante esta *Ley* se le ordenó al Comité:

- Crear el *Protocolo para Garantizar la Comunicación Efectiva entre los Componentes de Seguridad del Estado Libre Asociado de Puerto Rico* (*Protocolo*). Este consistirá de un conjunto de normas y procedimientos uniformes para permitir el intercambio efectivo de información entre las entidades gubernamentales de seguridad pública. Este *Protocolo* debía ser aprobado luego de transcurridos 90 días desde la aprobación de la *Ley* y de ser remitido a la Asamblea Legislativa.

- Rendir un informe detallado del plan de trabajo para implementar las medidas dispuestas en la mencionada *Ley*, dentro de un término no mayor de 30 días, luego de haberse organizado el Comité. Además, remitir copia de este informe a la Asamblea Legislativa.

El examen relacionado con las operaciones del *Comité* reveló que no había realizado las siguientes tareas necesarias para el funcionamiento efectivo del SIJC:

1) Al 17 de mayo de 2018, no se había aprobado ni enviado a la Asamblea Legislativa el *Protocolo*. Esto, luego de haber transcurrido 1,360 días desde el 26 de agosto de 2014, fecha de aprobación de la *Ley*.

2) Al 17 de mayo de 2018, no se había aprobado, ni remitido a la Asamblea Legislativa, el plan de trabajo para implementar las medidas dispuestas en la *Ley*. Habían transcurrido 1,361 días desde el 27 de agosto de 2014, fecha de la primera reunión del Comité, y solo se contaba con un borrador del plan.

Criterio

Las situaciones comentadas se apartan de lo establecido en los artículos del 5 al 7 de la *Ley 143-2014*.

Efectos

Las situaciones comentadas no permiten al Comité realizar una planificación ágil y adecuada para permitir el intercambio efectivo de información entre las entidades gubernamentales de seguridad pública. Además, la situación comentada en el **apartado a.2)** no le permitía al Comité establecer las políticas y los controles que debía implementar el director administrativo para la operación adecuada del SIJC. **[Hallazgos del 2 al 6]**

Causas

La situación comentada en el **apartado a.1)** se debía a que el Comité no había obtenido una asignación de fondos de $105,000 de la Asamblea Legislativa de Puerto Rico para llevar a cabo una evaluación tecnológica que permita identificar la infraestructura de comunicación, el equipo, el personal, y la programación, y los problemas estructurales que pudieran afectar la integración de la información de las agencias. Además, no

había considerado la posibilidad de utilizar empleados de las entidades representadas en el Comité, para realizar la evaluación tecnológica necesaria para establecer el *Protocolo*.

La situación comentada en el **apartado a.2)** se debía a que, al no contar con la evaluación tecnológica, el Comité determinó referir el borrador para la evaluación y consideración de los nuevos miembros que ocuparían cargos a partir de enero de 2017.

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, lo siguiente:

> En la próxima reunión del Comité Intergubernamental se le expondrá a sus miembros la posibilidad de acoger oficialmente el sistema de Registro Criminal Integrado (RCI) como la plataforma de intercambio de datos entre todas las agencias que integran el mencionado Comité. Actualmente el RCI ya integra, comparte y disemina información, tal y como se aspiraba en la Ley 143 de 2014. De la misma forma y cónsono con ello, se les presentará un borrador del Protocolo y un plan de trabajo para formalizar la integración de las comunicaciones entre las agencias que componen el Comité. Los borradores serán evaluados por el Comité para aprobación final.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Atraso en la validación de los registros migrados al RCI

Situación

a. El RCC fue el sistema de registros criminales administrado y utilizado por el SIJC desde 1987 hasta el 2013. Este sistema estaba estructurado en una base de datos relacional[10] y fue sustituido por el RCI. La implementación del RCI incluyó la migración de 338,000 registros del RCC, realizada el 3 de noviembre de 2013.

   En el RCI se registran las etapas procesales, desde la vista preliminar hasta la lectura de sentencia, de los casos de delitos graves y los menos graves asociados a estos, que eran atendidos en los tribunales.

[10] Se compone de tablas que guardan datos y que se relacionan entre sí mediante una clave primaria o código de identificación única, lo que facilita el manejo de los mismos y la extracción de la información.

A partir del 2015, la expedición del *Certificado de Antecedentes Penales* (*Certificado*) se realiza desde el RCI[11]. El *Certificado* puede solicitarse personalmente en el Cuartel General o en las comandancias de área de la Policía, mediante el formulario *Solicitud de Certificado de Antecedentes Penales* (PPR-326), o a través de la página en Internet: www.pr.gov. Para solicitar dicho *Certificado* a través de Internet, se validaba la información del solicitante mediante su número de licencia de conducir o una identificación emitida por el Departamento de Transportación y Obras Públicas (DTOP)[12]. Las solicitudes que no podían ser procesadas a través del RCI por falta de información o por errores de validación en los registros, o que no podían ser corroboradas a través del sistema del DTOP, se enviaban a la Sección de Análisis de la División de Emisión de Certificado de Antecedentes Penales de la Policía para su evaluación.

El SIJC atendía las solicitudes de los ciudadanos para eliminar en sus certificados de antecedentes penales las sentencias de culpabilidad que habían cumplido con los requisitos de ley. Además, atendía las solicitudes para eliminar de los certificados las sentencias de culpabilidad que surgían por casos de robo de identidad, o por la falta de actualización en el RCI de las sentencias eliminadas a través del sistema ANPE de la Policía, mediante el cual se generaban anteriormente los certificados[13].

Nuestro examen sobre la migración de los registros del RCC al RCI reveló que al 21 de septiembre de 2016, no se habían validado 300,000 (89%) de los 338,000 registros migrados. Esto, luego de haber transcurrido 1,053 días desde la fecha de la migración.

---

[11] Anteriormente, los certificados de antecedentes penales se emitían a través del Sistema de Expedición de Certificado de Antecedentes Penales (ANPE) de la Policía.

[12] El RCI validaba la identidad de los solicitantes con la información de la base de datos del DTOP.

[13] En estos casos los ciudadanos debían volver a solicitar la eliminación de las convicciones, aun cuando ya habían realizado el proceso para que se eliminaran del sistema ANPE.

Esta validación era necesaria para corregir los registros erróneos y los no migrados. A la fecha de nuestro examen, las validaciones se realizaban conforme a las solicitudes de los ciudadanos.

Criterio

La situación comentada es contraria a lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta de Circular 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*[14], aprobada el 8 de diciembre de 2004 por la directora de la Oficina de Gerencia y Presupuesto (OGP). En esta se establece que las agencias deben implementar metodologías para asegurar la integridad y confiabilidad de los datos producidos y almacenados. Esta política se implementa, en parte, mediante la validación de los datos registrados o migrados al RCI. Esto, para asegurar que dicho sistema contenga la información completa, correcta y actualizada de los convictos, los delitos cometidos, y las sentencias y convicciones.

Efectos

La situación comentada afecta la integridad del RCI, debido a que la información almacenada en este no estaba completa y correcta. Además, ocasiona demoras y contratiempos a los ciudadanos que solicitan el *Certificado*. También impide al SIJC establecer una fecha estimada para completar el proyecto de validación de los registros migrados del RCC, ya que, debido a la falta de integridad del RCI, el personal del SIJC asignado a realizar las validaciones ha tenido que dar prioridad a la atención de las reclamaciones de los ciudadanos que solicitan la eliminación de convicciones.

Causas

La situación comentada se debió a que el Departamento no había identificado los fondos necesarios para contratar los 10 empleados que el

---

[14] 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.

SIJC necesitaba para validar los registros migrados con errores del RCC. Además, las 3 especialistas de validación de récords debían atender las solicitudes de los ciudadanos relacionadas con errores en el *Certificado*.

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, lo siguiente:

> [...] al presente la validación y actualización de récords criminales se realiza conforme a las peticiones que presentan diariamente los ciudadanos para la eliminación de convicciones, peticiones que se realizan desde los estados y territorios de los Estados Unidos cuando una persona interesa comprar un arma de fuego (National Instant Criminal Background Check, NICS), peticiones que realizan las dependencias gubernamentales de Puerto Rico cuando interesan reclutar a un candidato para ocupar un puesto, peticiones que realiza la Policía de Puerto Rico para trabajar récords criminales sin disposición final (incompletos) y peticiones que realizan los funcionarios de las Fiscalías de Puerto Rico para completar o corregir records de personas procesándose criminalmente, así como información relacionada a la adición de las etapas de los programas de desvío y los indultos. De la misma forma, cuando la Administración de los Tribunales (OAT) y la Junta de Libertad Bajo Palabra (JLBP) ingresan órdenes de arresto al sistema y algún dato requiere validación, o cuando algún estado o territorio de los Estados Unidos solicita que se complete la disposición final de un caso criminal [...]. [*sic*]
>
> Como medida de acción correctiva para atender este hallazgo, el SIJC-PR continuará realizando las gestiones afirmativas para que la Secretaría Auxiliar de Recursos Humanos del Departamento de Justicia identifique el personal necesario **y se hagan las gestiones correspondientes con** la Oficina de Administración y Trasformación de Recursos Humanos (OATRH) para que supla la necesidad de la agencia mediante mecanismos de traslados o movilidad a tenor con la Ley Núm. 8-2017. Además, se llevará la situación a la atención de los funcionarios que componen el Comité Intergubernamental, a los fines de auscultar la posibilidad de que se destaque en el SIJC-PR personal de las agencias que dirigen o representan. También, se impartieron instrucciones a la Directora de Recursos Externos para la identificación de los fondos necesarios para poder cubrir las necesidades de la falta de personal del SIJC-PR. [*sic*]

Véase la Recomendación 3.a.

Hallazgo 3 - Falta de un plan de continuidad de negocios, un plan de contingencias sobre los sistemas de información, un centro alterno para la recuperación de las operaciones computadorizadas, y copias de respaldo fuera de las instalaciones del SIJC

Situaciones

a. Al 25 de abril de 2016, el SIJC carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de sus operaciones. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red de comunicación o desastres naturales, entre otros.

b. Al 25 de abril de 2016, el SIJC carecía de un plan de contingencias para los sistemas de información, aprobado, que incluyera los siguientes requisitos para atender situaciones de emergencia:

- Los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información de los usuarios que acceden los sistemas de información mediante conexiones remotas
- El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones
- La identificación de los archivos críticos del SIJC
- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
- El detalle de la configuración de los equipos críticos (equipo de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
- El nombre del encargado de activar el plan y del personal de reserva, de forma tal que pueda ser ejecutado sin depender de individuos específicos

- Una hoja de cotejo para verificar los daños ocasionados por la contingencia
- Una lista de los números de teléfono de los miembros de cada grupo de recuperación.

c. Al 22 de abril de 2016, el SIJC no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

d. Al 22 de octubre de 2016, en el SIJC no se preparaban copias de los respaldos realizados para enviarlos y mantenerlos fuera de sus instalaciones. Los respaldos se realizaban diariamente y permanecían en el servidor donde se preparaban.

Situaciones similares a las mencionadas en los **apartados b. y c.** se incluyeron en el *Informe de Auditoría TI-05-07* del 3 de diciembre de 2004.

Criterios

Las situaciones comentadas en los **apartados a. y d.** son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 77-05*. En esta se establece que las agencias gubernamentales deben desarrollar un plan de continuidad de negocios, que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones. Además, establece que deben existir procedimientos para tener y mantener una copia de respaldo recurrente de la información, y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones de la entidad. En consonancia con dicha política pública es necesario, entre otras cosas, que toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro, fuera de los predios de la entidad. Esto, con el propósito de recuperar la mayor cantidad de información posible en caso de una emergencia o desastre.

Las mejores prácticas en el campo de la tecnología de información 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 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 debe estar aprobado por el funcionario de máxima autoridad de la agencia e 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.]**

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 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.** podrían 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 a los usuarios y a los clientes del SIJC. Además, ocasionaron que el SIJC estuviera desprovisto de medidas de contingencia necesarias para proteger los equipos en situaciones de averías como las comentadas en el **Hallazgo 4**, lo que pone en riesgo sus operaciones.

La situación comentada en el **apartado c.** podría afectar las operaciones del SIJC, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afecte su funcionamiento.

Las situaciones comentadas en los **apartados c. y d.** impiden el pronto restablecimiento de las operaciones normales del SIJC después de una emergencia o evento que afecte su funcionamiento.

Causas

Las situaciones comentadas en los **apartados a. y b.** se debieron a que el Comité entendía que antes de desarrollar el plan de continuidad era necesario realizar la evaluación tecnológica de las entidades adscritas a este.

Las situaciones comentadas en los **apartados c. y d.** se debieron a que en la División de Recursos Externos del Departamento no se habían identificado los fondos necesarios para el establecimiento de un centro alterno, y para la adquisición de las herramientas tecnológicas que eran necesarias para preparar las copias de los respaldos.

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, las medidas que están en proceso para corregir las situaciones comentadas.

Véanse las recomendaciones 3 de la b. a la e., y 4.

Hallazgo 4 - Incidente relacionado con el acondicionador de aire del Centro de Datos, que puso en riesgo la continuidad de las operaciones del SIJC

Situación

a. El Centro de Datos del SIJC contaba con una unidad de acondicionador de aire marca APC, modelo FM-50, que fue adquirida el 31 de octubre de 2007 a un costo de $45,631. Según la documentación técnica del proveedor, los compresores de esta unidad tenían una vida útil estimada de 15 años, y contaba con un sistema de advertencias preventivas para alertar sobre sus fallas.

De acuerdo con los registros, los últimos servicios de inspección y diagnóstico que recibió la unidad fueron ofrecidos el 12 de agosto de 2013 y el 29 de julio de 2014 por una compañía externa. Estos servicios fueron requisados mediante dos órdenes de compra, ascendentes a $1,200.

El 4 de octubre de 2015 la unidad se averió y estuvo fuera de servicio hasta el 11 de mayo de 2016. Durante los siete meses de la avería, el director administrativo del SIJC improvisó medidas de contingencia para permitir el flujo del aire y bajar la temperatura del Centro de Datos, que incluyeron mantener abiertas las puertas de acceso al área y usar abanicos eléctricos. Durante el incidente, el SIJC estuvo desprovisto del sistema de alarma del acondicionador de aire que alertaba sobre la necesidad de apagar los equipos para protegerlos de altas temperaturas. Los discos de los servidores instalados en la nube fueron remplazados mediante garantía, y no se invirtió en la reparación del otro servidor, debido a que no era costo-efectivo, por ser un equipo obsoleto.

El Departamento invirtió $1,587 en servicios para la reparación de los motores de la unidad de acondicionador de aire averiada, que extendían su vida útil por cinco años.

Criterios

La situación comentada es contraria a lo establecido en el *Reglamento de Seguridad y Privacidad del Sistema de Información de Justicia Criminal*, aprobado en el 1996. En este se establece que la Junta Ejecutiva[15], el director administrativo y el grupo técnico son responsables de la protección del equipo físico y del almacenamiento de los diferentes bancos de datos creados en el SIJC para impedir daños, perdida, alteración y mutilación de la información.

[15] A la fecha de nuestra auditoría, la Junta Ejecutiva había sido remplazada por el Comité Interagencial. Sin embargo, este *Reglamento* continuaba vigente.

Además, la situación comentada se aparta de lo establecido en la *Política TIG-003* y en la *Política TIG-004, Servicios de Tecnología,* de la *Carta Circular 77-05*; y de la *Política TIG-015, Programa de Continuidad Gubernamental*[16], aprobada el 22 de septiembre de 2011 por el director de la OGP. Es estas se establece que:

- Cada agencia debe implementar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada o maliciosa. Para esto, debe llevar a cabo un análisis de riesgos que servirá de base para desarrollar un plan de continuidad de negocios que incluya un plan para recuperación de desastres y un plan para la continuidad de las operaciones. **[Política TIG-003]**
- El personal de la oficina de tecnologías de información de la agencia es responsable del mantenimiento de sus sistemas internos y los revisará regularmente para verificar que funcionen adecuadamente. **[Política TIG-004]**
- La agencia es responsable de asegurar la continuidad de sus operaciones mediante un plan de recuperación por desastre desarrollado de acuerdo a la política de seguridad. **[Política TIG-015]**

Efecto

Como consecuencia de la situación comentada, se dañaron los discos del servidor en el que se mantenían los datos del *Prossecution Case Management System (PCMS)*, de la Secretaría Auxiliar de Asuntos de Menores y Familia, y del RCC; y dos discos de los servidores instalados en la unidad de nube. Esto, a su vez, ocasionó que se afectaran las funciones de balance de carga (*load balance)* entre los ocho servidores que maneja el RCI, y se limita la capacidad de operación de este sistema.

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

Además, ocasionó la pérdida de los datos del *PCMS* y del RCC y puso en riesgo la continuidad de las operaciones del SIJC y los equipos del Centro de Datos que tenían un costo estimado de $767,500.

Causas

La situación comentada se debió a que, por limitaciones presupuestarias, el director administrativo del SIJC no había establecido un plan de mantenimiento preventivo y de remplazo para la unidad de acondicionador de aire. Además, se debe a que el Departamento tardó cuatro meses en completar el proceso de la orden de compra para el remplazo y mantenimiento del acondicionador de aire, y luego el proceso se interrumpió debido a un cambio en precio[17] de la propuesta presentada por el proveedor.

Además, a la fecha del incidente, el SIJC no contaba con un plan de continuidad de operaciones ni con un plan de contingencias que incluyera los procedimientos a seguir para atender situaciones relacionadas con el acondicionador de aire, el daño de los discos y la pérdida de información. **[Véase el Hallazgo 3-a. y b.]**

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, las medidas que están en proceso para corregir la situación comentada. Entre estas, el plan para ubicar el Centro de Datos del SIJC en el las nuevas instalaciones del Departamento, que cuenta con dos unidades centrales de acondicionador de aire.

Véanse las recomendaciones 3.b. y f., y 4.

---

[17] El 31 de marzo de 2016 el proveedor notificó al Departamento un cambio en el costo de la propuesta inicial de $76,503, debido a la necesidad de modificar el modelo, por la distancia que existía entre la unidad interior (manejadora) y la unidad exterior (condensadora). El precio por el modelo revisado se estableció en $91,519. A esa misma fecha, presentó otra cotización por $1,587 para los servicios de reparación de los motores de la unidad de aire acondicionado averiada, que extendía por cinco años la vida útil de los motores.

Hallazgo 5 - Accesos al SORNA otorgados a empleados del DCR que no lo utilizaban, y falta de revisiones de las transacciones realizadas por sus usuarios y los del RCI

Situaciones

a. El SORNA era utilizado por personal de la Policía de Puerto Rico, del Departamento de Corrección y Rehabilitación (DCR), del Departamento de Justicia, y de otras agencias federales relacionadas con la seguridad y el orden público.

El supervisor de operaciones de procesamiento de datos y el director de análisis y programación de sistemas de información del SIJC eran responsables de crear, modificar y eliminar los accesos a la red y al SORNA. Estos eran supervisados por el director administrativo del SIJC. Además, en cada agencia se nombraba un *Terminal Agency Coordinator* (TAC). Estos tramitaban al SIJC el *Formulario para Solicitar Cuenta para Acceso al Registro de Ofensores Sexuales y/o Maltrato de Menores*. También supervisaban a los usuarios para asegurarse de que cumplieran con el *Criminal Justice Information Services (CJIS) Security Policy,* aprobado el 9 de febrero de 2011 por el *CJIS Advisory Policy Board*, el cual regía las operaciones del SIJC.

Los privilegios para acceder al SORNA incluían:

- Admin - Permitía acceder a todas las funciones del sistema, validar la información registrada por los usuarios con rol *Standard* y modificar la información de la página en Internet para, entre otras cosas, mostrar o no la información de los convictos. Este acceso era otorgado a los usuarios que realizaban funciones relacionadas con la administración del SIJC.

- *Standard* - Permitía añadir y editar la información de los convictos, y producir informes. Este acceso era otorgado a los empleados de la Policía de Puerto Rico que eran los responsables de la creación y el seguimiento de los casos registrados en el SORNA.

- *Read Only* - Permitía ver la información registrada en el sistema.

Examinamos los privilegios de acceso otorgados a 24 de las 275 cuentas activas en el SORNA, al 19 de diciembre de 2016, y realizamos entrevistas, entre el 21 de febrero y el 20 de abril de 2017, al personal que laboraba en el SIJC, el DCR, la Policía de Puerto Rico y el Programa de Servicios de Antelación al Juicio del DCR (PSAJ). El examen realizado reveló que a 16 empleados del DCR, que fueron entrevistados, se les había otorgado acceso al SORNA, a pesar de que estos no utilizaban dicho sistema. De estos empleados, 3 tenían asignados accesos con privilegios *Standard* y 13 con *Read Only*. La revisión del registro de las transacciones realizadas por los usuarios del SORNA entre el 1 de diciembre de 2015 y el 31 de mayo de 2016, que nos proveyó el SIJC, reflejó que estos empleados no realizaron transacciones en el sistema.

b. Al 1 de junio de 2017, en el SIJC no se revisaban los registros de las transacciones realizadas por los usuarios del RCI y el SORNA, como parte de un proceso de supervisión y de control interno.

Criterios

Las situaciones comentadas se apartan de lo establecido en la *Política ATI-003, Seguridad de los Sistemas de Información,* de la *Carta Circular 140-16*. En esta se establece que las entidades gubernamentales deberán establecer controles adecuados para la utilización de las aplicaciones, de tal manera que solo el personal autorizado pueda ver los datos y acceder a las aplicaciones que necesite utilizar. Además, que los privilegios de acceso deben ser evaluados regularmente, y que deben existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos que lo ameriten. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades.

Además, las situaciones comentadas son contrarias a lo establecido en la *Sección 5.5.2.1 Policy Area 5:Access Control* del *CJIS Security Policy*. En esta se establece que:

> The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain and review records reflecting such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specific task. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Efecto

La situación comentada en el **apartado a.** puede propiciar que se realicen modificaciones no autorizadas en el SORNA, y comprometer la confidencialidad de los datos personales que se mantienen en el mismo, sin que esto pueda ser detectado a tiempo para fijar responsabilidades.

Lo comentado en el **apartado b.** impide la detección oportuna de accesos o alteraciones no autorizadas de la información contenida en los sistemas del SIJC.

Causas

La situación comentada en el **apartado a.** se debió a que el SIJC no había implementado un procedimiento para evaluar regularmente la necesidad de los accesos otorgados a los usuarios. Tampoco había implementado un procedimiento para que los TAC asignados en las agencias informaran sobre los cambios de personal que requerían modificar o eliminar los accesos.

La situación mencionada en el **apartado b.** se debía a que el SIJC no contaba con personal suficiente para poder asignar la función de supervisión o revisión de todas las transacciones de los usuarios.

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, las medidas que están en proceso para corregir la situación comentada en el **apartado b.**

Véase la Recomendación 3.g. y h.

Hallazgo 6 - Falta de una metodología formal para la adquisición y el desarrollo de aplicaciones

Situación

a. Al 4 de octubre de 2016, el SIJC no había establecido una metodología formal para la adquisición y el desarrollo de aplicaciones que considerara, entre otras cosas, lo siguiente:

- La documentación de la justificación de la inversión en el proyecto de adquisición o desarrollo
- Un estudio de viabilidad que describa las ventajas y desventajas operacionales y el análisis de costo-beneficio de cada opción
- La aprobación para el inicio del desarrollo de los sistemas e implementación de las aplicaciones
- La documentación adecuada que se requiere para cada fase del desarrollo de aplicaciones, y los manuales de operaciones y de los usuarios
- La capacitación de los usuarios
- Las especificaciones de la programación y el equipo
- Los requerimientos de las pruebas y los resultados
- Los procedimientos de contratación que incluyeran, entre otros, la descripción de los productos esperados del proyecto, tales como: componentes y códigos fuente del sistema, marcos de tiempo del proyecto, horas calculadas y gasto máximo permisibles para cada fase.

Criterio

La situación comentada se aparta de lo establecido en la *Política TIG-011* de la *Carta Circular 77-05*. En esta se establece, como política pública, que la planificación, el diseño, la adquisición y la implementación de proyectos de tecnología son guiados por unos principios para apoyar la estrategia de gobierno, sus metas y objetivos. Como parte de estos principios, toda aplicación comercial o personalizada implementada debe

ser evidenciada mediante metodologías de desarrollo y documentación estándar o de uso común. Esto contribuye a asegurar que los diseñadores de sistemas cumplan con los requerimientos de los usuarios del sistema y los requisitos organizacionales; se mantenga la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia; se realice un mantenimiento a la aplicación rápido, efectivo y eficiente; y se facilite la labor de adiestramiento.

Efectos

La situación comentada podría ocasionar que los procesos de adquisición e implementación de los sistemas de información computadorizados no se realicen de manera uniforme. Esto, podría reducir la efectividad de los mismos, y que los sistemas no se ajusten a las necesidades de los usuarios ni a la infraestructura establecida, y no sean costo-efectivos para el SIJC.

Causa

La situación comentada se atribuye a que el director administrativo del SIJC desconocía sobre los principios que rigen la planificación, el diseño y el desarrollo de proyectos de tecnología, y las metodologías formales de este proceso. Además, el Comité no le requirió que redactara y remitiera para su consideración y aprobación, los procedimientos para documentar la metodología a seguir en los procesos de adquisición y desarrollo de aplicaciones, y en la administración de los proyectos del SIJC.

Comentarios de la Gerencia

La secretaria de Justicia nos indicó, entre otras cosas, las medidas que están en proceso para corregir la situación comentada.

Véase la Recomendación 3.i.

RECOMENDACIONES

A la Secretaria de Justicia y Presidenta del Comité Intergubernamental

1. Coordinar con los miembros del Comité para que se realice la evaluación tecnológica necesaria para establecer el *Protocolo* requerido en la *Ley 143-2014*. Considerar la posibilidad de utilizar personal de las agencias representadas en el Comité para que realicen la evaluación técnica de sus infraestructuras de comunicación,

equipos, personal y programación, así como de los problemas estructurales que afectan la integración de los datos entre los departamentos y las agencias que representan. **[Hallazgos 1-a.1)]**

2. Realizar las gestiones necesarias para que el Comité evalúe y apruebe el borrador del plan de trabajo para el SIJC, y supervise la ejecución del mismo para mantener un control adecuado de sus operaciones. **[Hallazgo 1-a.2)]**

3. Ejercer una supervisión eficaz sobre el director administrativo del SIJC para asegurarse de que:

   a. De seguimiento al proceso de solicitud de asignación de personal necesario en el SIJC para completar la validación de los registros migrados al RCI. Considere la posibilidad de que se asignen empleados de otras agencias bajo las disposiciones de empleador único establecidas en la *Ley 8-2017*, *Ley para la Administración y Transformación de los Recursos Humanos en el Gobierno de Puerto Rico*, según enmendada. **[Hallazgo 2]**

   b. Prepare y remita, para la aprobación del Comité, un plan de continuidad de negocios que incluya los planes específicos, completos y actualizados de la SIJC para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar sus operaciones, en caso de emergencia. Una vez este documento sea aprobado, tome las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios del SIJC. Además, se asegure de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgos 3-a. y 4]**

   c. Prepare y remita, para su aprobación, un plan de contingencias detallado para el SIJC, en el que se establezcan las medidas a considerarse en caso de ocurrir eventos o situaciones de

emergencia que afecten sus operaciones, tales como: interrupciones de energía eléctrica, errores humanos, terremotos o fuegos, entre otros, y que incluya los aspectos comentados en el **Hallazgo 3-b.**

d. Identifique como centro alterno un lugar que sea costo efectivo, que no esté expuesto a los mismos riesgos que el SIJC, y que cuente con la infraestructura y los equipos necesarios para restaurar sus operaciones críticas, en caso de emergencia. Además, si el lugar identificado como centro alterno está localizado en otra entidad, realice las gestiones que permitan formalizar acuerdos que sean necesarios para utilizar el mismo. 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 3-c.]**

e. Realice, en coordinación con la directora de recursos externos del Departamento, las gestiones necesarias para adquirir los equipos y medios de almacenaje que sean necesarios para realizar las copias de respaldo de información almacenada en los servidores del SIJC, y los almacene y retenga en un lugar externo. **[Hallazgo 3-d.]**

f. Se asegure que se establezca y coordine un plan de mantenimiento preventivo para las unidades de acondicionador de aire que proveerán servicio al Centro de Datos en las nuevas instalaciones del Departamento. **[Hallazgo 4]**

g. Establezca un procedimiento para evaluar regularmente la necesidad y utilidad de los accesos otorgados a los usuarios del SORNA, de manera que se corrijan las situaciones mencionadas en el **Hallazgo 5-a.**

h. Establezca un procedimiento para revisar, mediante muestreo, las transacciones realizadas por los usuarios del RCI y el

SORNA, y asigne al técnico de operaciones para que las revise. Además, evalúe la posibilidad de solicitar recursos adicionales al Departamento para realizar estas revisiones. **[Hallazgo 5-b.]**

i. Establezca una metodología formal para la planificación, el diseño, la adquisición y la implementación de proyectos de tecnología conforme a la *Política ATI-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 140-16*, y las mejores prácticas en el campo de la tecnología de información. **[Hallazgo 6]**

4. Ver que la directora de recursos externos identifique y asigne los fondos necesarios para corregir las situaciones comentadas en los **hallazgos 3.c. y d., y 4**.

APROBACIÓN

A los funcionarios y a los empleados del SIJC, 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: Yamín M Calaf Irizarry

ANEJO 1

DEPARTAMENTO DE JUSTICIA
SISTEMA DE INFORMACIÓN DE JUSTICIA CRIMINAL

MIEMBROS PRINCIPALES DEL COMITÉ INTERGUBERNAMENTAL DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Wanda Vázquez Garced	Presidenta	9 ene. 17	15 jun. 17
Lcdo. César R. Miranda Rodríguez	Presidente	25 ene. 16	31 dic. 16
Hon. Sigfrido Steidel Figueroa	Director Administrativo de los Tribunales	6 sep. 16	15 jun. 17
Hon. Isabel Llompart Zeno	Directora Administrativa de los Tribunales	25 ene. 16	2 sep. 16
Cnel. Michelle Hernández de Fraley	Superintendente de la Policía	9 ene. 17	15 jun. 17
Cnel. José L. Caldero López	"	25 ene. 16	31 dic. 16
Hon. Erick Rolón Suárez	Secretario de Corrección y Rehabilitación	9 ene. 17	15 jun. 17
Lcdo. Einar Ramos López	"	25 ene. 16	15 dic. 16
Hon. Glorimar Andújar Matos	Secretaria de la Familia	2 ene. 17	15 jun. 17
Sra. Idalia Colón Rondón	"	25 ene. 16	31 dic. 16
Hon. Carlos Contreras Aponte	Secretario de Transportación y Obras Públicas	3 ene. 17	15 jun. 17
Ing. Miguel A. Torres Díaz	"	25 ene. 16	31 dic. 16
Dr. Edwin Crespo Torres	Director del Instituto de Ciencias Forenses	1 jun. 17	15 jun. 17
Dra. Edda Rodríguez Morales	Directora del Instituto de Ciencias Forenses	25 ene. 16	31 dic. 16

ANEJO 2

DEPARTAMENTO DE JUSTICIA
SISTEMA DE INFORMACIÓN DE JUSTICIA CRIMINAL

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Wanda Vázquez Garced	Secretaria de Justicia	9 ene. 17	15 jun. 17
Lcdo. César R. Miranda Rodríguez	Secretario de Justicia	25 ene. 16	31 dic. 16
Ing. Heriberto Luna de los Santos	Director Administrativo del SIJC	25 ene. 16	15 jun. 17
Sra. Lillian Sánchez Pérez	Secretaria Auxiliar de Gerencia y Administración	16 feb. 17	15 jun. 17
Sr. Alwin Miranda Rodríguez	Secretario Auxiliar de Gerencia y Administración Interino	2 ene. 17	15 feb. 17
Sra. Waleska Rosario Rodríguez	Secretaria Auxiliar de Gerencia y Administración	1 jul. 16	22 dic. 16
CPA Dania R. Frías Martínez	"	25 ene. 16	30 jun. 16
CPA Dania R. Frías Martínez	Directora de Finanzas[18]	1 jul. 16	15 jun. 17
Sra. Mariela Cabán Torres	Directora de Recursos Externos[19]	16 mar. 16	15 jun. 17
Sr. José V. Alvarado Martínez	Secretario Auxiliar de Recursos Humanos	16 feb. 17	15 jun. 17
Lcdo. William Machado Aldarondo	Secretario Auxiliar de Recursos Humanos Interino	1 ene. 17	15 feb. 17
Lcda. Jeannette M. Negrón Ramírez	Secretaria Auxiliar de Recursos Humanos	25 ene. 16	31 dic. 16

[18] El puesto de director de finanzas estuvo vacante del 25 de enero al 30 de junio de 2016.

[19] El puesto de director de recursos externos estuvo vacante desde el 25 de enero al 15 de marzo de 2016.

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-18-19* del 27 de abril de 2018, disponible en nuestra página en Internet.

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr