INFORME DE AUDITORÍA TI-15-09

1 de mayo de 2015

Policía de Puerto Rico

Negociado de Tecnología y Comunicaciones

División de Tecnología

(Unidad 5386 - Auditoría 13784)

Período auditado: 8 de octubre de 2012 al 20 de diciembre de 2013

CONTENIDO

Página

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

1 de mayo de 2015

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

Realizamos una auditoría de las operaciones de la División de Tecnología del Negociado de Tecnología y Comunicaciones (NTC) de la Policía de Puerto Rico (Policía) 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 8 de octubre de 2012 al 20 de diciembre de 2013. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este es el segundo informe, y contiene cinco hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para el acceso lógico y físico, y las redes de comunicación. Además, contiene un comentario especial relacionado con la inversión de fondos públicos en la implantación de proyectos de tecnología para computadorizar las patrullas de la Policía. En el **ANEJO 1** presentamos información del primer informe

emitido sobre las operaciones de la División de Tecnología del NTC de la Policía. Ambos están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Policía es un organismo civil cuya responsabilidad es proteger a las personas y a la propiedad; mantener y conservar el orden público; observar y procurar la protección de los derechos civiles del ciudadano; prevenir, descubrir, investigar y perseguir el delito; y, dentro de la esfera de sus atribuciones, compeler obediencia a las leyes y ordenanzas municipales y a los reglamentos que conforme a estas se promulgan. Esto, mediante la *Ley 53-1996*, *Ley de la Policía de Puerto Rico de 1996*, según enmendada, la cual derogó la *Ley Núm. 26 del 22 de agosto de 1974*, *Ley de la Policía de Puerto Rico de 1974*, según enmendada. La *Ley 53-1996* se adoptó con el propósito de darle uniformidad a la estructura operacional de la Policía para hacer más ágil su administración y la utilización de sus recursos.

El Gobernador ejerce la autoridad suprema en cuanto a la dirección de la Policía, pero la administración y la dirección inmediata de la organización se delegaron, por ley, en el Superintendente. Este es nombrado por el Gobernador, con el consejo y consentimiento del Senado. Del 8 de octubre de 2012 al 15 de noviembre de 2013, el puesto de Superintendente estuvo ocupado por el Sr. Héctor M. Pesquera López, mediante destaque administrativo de la Autoridad de Puertos del Condado de Miami Dade de la Florida. Este destaque era parte del acuerdo interagencial formalizado mediante el Contrato 2012-000041 del 12 de marzo de 2012, entre el Gobierno del Estado Libre Asociado de Puerto Rico y el Condado de Miami Dade, para obtener servicios profesionales relacionados con la seguridad pública. El contrato incluía servicios para requerir consejo, recursos humanos y asistencia técnica en asuntos de seguridad, tenía vigencia del 2 de abril de 2012 al 1 de abril de 2013; y un costo de $283,100. Posteriormente, se formalizaron los contratos 2013-000052, 2013-000053 y 2014-000025 por $69,671, $23,223 y $46,447, respectivamente. El período cubierto por estos contratos fue del 1 de abril al 31 de agosto de 2013.

El 2 de septiembre de 2013 el Gobernador firmó el *Boletín Administrativo OE-2013-063, Orden Ejecutiva del Gobernador del Estado Libre Asociado de Puerto Rico Hon. Alejandro J. García Padilla, para Crear el Cargo de Principal Oficial en Asuntos de Seguridad Pública de Puerto Rico*. Este cargo está adscrito a la Oficina del Gobernador y ejerce las funciones del Superintendente de la Policía[1]. El señor Pesquera López ocupó este puesto del 2 de septiembre al 15 de noviembre de 2013. Del 1 de diciembre de 2013 al 31 de marzo de 2014, el puesto fue ocupado por el Sr. James Tuller Cintrón.

La estructura organizacional de la Policía estaba compuesta por la Oficina del Superintendente; las superintendencias auxiliares[2] de Operaciones Estratégicas, Responsabilidad Profesional, Relaciones con la Comunidad, Servicios al Ciudadano, Servicios Administrativos, Servicios Gerenciales y Operaciones de Campo; y las oficinas de Asuntos Legales, Auditoría Interna, Fuerzas Conjuntas, Prensa, Seguridad de la Fortaleza, y Seguridad y Protección. Además, contaba con 4 regiones (Norte, Sur, Este y Oeste)[2], 13 áreas policíacas, 68 distritos, 38 precintos, el Colegio Universitario de Justicia Criminal de Puerto Rico (CUJC) y la Oficina de Fuerzas Unidas de Rápida Acción (FURA).

El NTC se creó mediante la *Orden General 2009-1* del 24 de febrero de 2010 y estaba adscrito a la Superintendencia Auxiliar de Servicios Administrativos[2]. El propósito de esta orden era establecer nuevos cambios a la estructura organizacional y funcional en la Policía para lograr una mayor efectividad y eficiencia administrativa y operacional, conforme a lo establecido en la *Ley 53-1996*. El NTC era responsable de planificar,

---

[1] La *Orden Ejecutiva* está vigente. Sin embargo, el cargo de Principal Oficial en Asuntos de Seguridad Pública de Puerto Rico no ha sido ocupado luego del 31 de marzo de 2014.

[2] Al 1 de mayo de 2014, la Policía contaba con las superintendencias auxiliares de Operaciones de Campo, Investigaciones Criminales, Responsabilidad Profesional, Servicios Gerenciales, Policía de Fortaleza, y Educación y Adiestramiento. El número de oficinas se redujo a tres: Asuntos Legales, Prensa y Reforma. A esa fecha también se habían eliminado las cuatro regiones. Además, se eliminó la Superintendencia Auxiliar de Servicios Administrativos y sus negociados y divisiones fueron transferidos a la Superintendencia Auxiliar de Servicios Gerenciales.

organizar, implantar y mantener los sistemas computadorizados de información y estaba compuesto por la División de Tecnología y la de Comunicaciones.

El objetivo de la División de Tecnología era ofrecer soluciones tecnológicas y confiables que permitieran a la Policía cumplir con su misión y sus objetivos; proveer todos sus servicios de tecnología con la mayor calidad posible; y cumplir con las expectativas de sus clientes.

A la fecha de nuestra auditoría, esta división era dirigida por un teniente, quien realizaba las funciones de Director Interino[3]. La División de Tecnología se componía de las siguientes áreas:

- Operaciones Centros de Cómputos - Contaba con 1 Supervisor de Operador de Equipos Electrónicos de Información, 3 operadores de computadoras y 1 Bibliotecario.
- Desarrollo de Aplicaciones - Contaba con tres programadores.
- *Service Desk* - Contaba con dos oficinistas de apoyo técnico.
- Infraestructura - Contaba con ocho empleados que realizaban tareas relacionadas con la instalación de infraestructura, el inventario de equipo y las redes de comunicaciones.

La División de Comunicaciones era responsable de planificar, diseñar, implantar, mantener y controlar toda la infraestructura de redes de comunicaciones de radio frecuencias. Esta era dirigida por una Directora y contaba con áreas responsables de las licencias de la *Federal Communications Comission* (FCC); la interoperabilidad de equipos de comunicación, y de los teléfonos celulares y satelitales; los sistemas troncalizados; los radios de portátiles; los servicios especiales[4]; y las microondas.

[3] El teniente realizó las tareas de Director Interino del 8 de octubre al 7 de diciembre de 2012. A partir del 13 de diciembre de 2012, estas tareas fueron asignadas al Supervisor de Operador de Equipos Electrónicos de Información.

[4] Esto incluye la operación de antenas y de las plantas eléctricas.

Para realizar sus funciones, la Policía contaba con 53 aplicaciones o sistemas computadorizados entre los que se encontraban los siguientes:

- *Crime Information Warehouse* (CIW) - Servía de repositorio de distintas bases de datos[5] y permitía la búsqueda de información para las investigaciones criminales.
- Sistema Automatizado de Identificación de Huellas Dactilares (AFIS) - Contenía el repositorio de huellas digitales y fotos de fichaje.
- Sistema de Expedición de Certificado de Antecedentes Penales (ANPE) - Contenía una relación de las sentencias condenatorias que aparecen en el expediente de cada persona que haya sido sentenciado en cualquier tribunal de justicia del Estado Libre Asociado de Puerto Rico y proveía el Certificado de Antecedentes Penales.
- Sistema de Registro de Armas y Municiones (FAS) - Contenía el registro de armas, licencias y municiones.
- Sistema *Positron Computer Aidded Dispatch* - Mantenía la información sobre las querellas recibidas en el Centro de Mando y permitía la asignación de agentes para la investigación de las querellas.
- Aplicación *Crime Mapping* - Contenía información de los delitos cometidos y permitía realizar búsquedas por tipo de delito, área, o día y hora en la que se cometieron los mismos. Además, desplegaba información en gráficas y en mapas de los sectores y precintos policíacos y los municipios de Puerto Rico.

[5] Provee información en tiempo real de las bases de datos de distintos sistemas, tales como: AFIS, ANPE, FAS, Positron, Crime Mapping, *Drivers and Vehicles Information Database Plus* (Sistema DAVID Plus) y el Departamento de Corrección y Rehabilitación.

Las transacciones de contabilidad de la Policía se procesaban mediante el *Puerto Rico Integrated Financial Administration System* (PRIFAS), mientras que las de nómina se procesaban mediante el sistema *Automated Data Processing* (ADP).

La Policía contaba con aproximadamente 5,000 computadoras y 54 servidores, de los cuales 30 eran virtuales, y tenía 3,410 usuarios con acceso a los sistemas de información (aplicaciones, sistemas, correo electrónico e Internet). Además, contaba con 16 redes virtuales de área local (VLAN, por sus siglas en inglés) y una red de área amplia (WAN, por sus siglas en inglés), para la comunicación de sus 139 redes de área local (LAN, por sus siglas en inglés) que corresponden al CUJC, las comandancias, los distritos, los precintos y las unidades especiales de la Policía.

Los recursos para financiar las actividades operacionales de la Policía provienen de fondos especiales estatales, federales y de estabilización; asignaciones especiales; otros ingresos; y la resolución conjunta del presupuesto general. Los gastos de operación del NTC eran sufragados del presupuesto del Programa de Dirección y Administración General, el cual para los años fiscales 2012-13 y 2013-14, ascendió a $6,030,000 y $5,864,000.

El **ANEJO 2** contiene una relación de los funcionarios principales de la Policía que actuaron durante el período auditado.

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

COMUNICACIÓN CON LA GERENCIA

La situación comentada en el **Hallazgo 4** de este *Informe* fue remitida al Sr. Héctor M. Pesquera López, entonces Superintendente de la Policía, mediante carta de nuestros auditores, del 13 de noviembre de 2013. Además, los **hallazgos 1 y del 3 al 5** de este *Informe*, se remitieron al Sr. James Tuller Cintrón, entonces Principal Oficial en Asuntos de

Seguridad Pública, y Superintendente Designado, mediante carta de nuestros auditores, del 17 de enero de 2014. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 21 de febrero de 2014, el señor Tuller Cintrón remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Dichos comentarios fueron considerados en la redacción del borrador de este *Informe*. El señor Pesquera López no contestó[6] la carta de nuestros auditores.

El borrador de seis hallazgos se remitió para comentarios al Cnel. José L. Caldero López, Superintendente de la Policía, por carta del 5 de febrero de 2015. En este se indicaron datos específicos, tales como: nombres de servidores y localización de áreas donde se mantenían los equipos de comunicación, los cuales por seguridad no se incluyen en este *Informe*.

Con el mismo propósito, remitimos el borrador de los seis hallazgos al señor Pesquera López, ex-Superintendente de la Policía, y al señor Tuller Cintrón, ex Principal Oficial en Asuntos de Seguridad Pública y Superintendente Designado, mediante cartas de esa misma fecha, por correo certificado con acuse de recibo. El borrador remitido al ex-Superintendente de la Policía se envió a una dirección provista por él, y el remitido al ex Principal Oficial en Asuntos de Seguridad Pública y Superintendente Designado, a una provista por la Oficina del Gobernador.

El 17 de febrero de 2015 el Dr. Juan C. Rivera Vázquez, Director del Negociado de Tecnología y Comunicaciones, en representación del Superintendente, solicitó una prórroga para remitir los comentarios al borrador de los hallazgos. El 18 de febrero le concedimos la prórroga hasta el 13 de marzo.

[6] El señor Pesquera López renunció al puesto de Superintendente el 15 de noviembre de 2013.

El 11 de marzo de 2015 se envió una carta de seguimiento al ex-Superintendente de la Policía y al ex Principal Oficial en Asuntos de Seguridad Pública y Superintendente Designado, y se les concedió hasta el 18 de marzo para remitir los comentarios al borrador de los **hallazgos** de este *Informe*.

El ex-Superintendente de la Policía y el ex Principal Oficial en Asuntos de Seguridad Pública y Superintendente Designado no contestaron el borrador de los hallazgos.

El Superintendente de la Policía contestó el borrador mediante carta del 13 de marzo. Luego de evaluar sus comentarios y la evidencia suministrada, determinamos que la Policía tomó las acciones correctivas pertinentes, excepto por los **hallazgos** que se incluyen en este *Informe*. En los **hallazgos** se incluyeron algunos de sus comentarios.

OPINIÓN Y HALLAZGOS

Opinión favorable con excepciones

Las pruebas efectuadas demostraron que las operaciones de la División de Tecnología del NTC de la Policía, en lo que concierne a controles internos establecidos para el acceso lógico y físico y las redes de comunicación, se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 5** que se comentan a continuación.

Hallazgo 1 - Falta de segregación de las funciones realizadas por el Supervisor de Operador de Equipos Electrónicos de Información y por los operadores de computadoras

Situación

a. Al 12 de septiembre de 2012, el Supervisor de Operador de Equipos Electrónicos de Información de la Policía realizaba las siguientes tareas correspondientes al puesto de un Administrador de Seguridad:

   1) Asignaba, activaba y eliminaba las cuentas de acceso a los usuarios de los sistemas computadorizados

   2) Creaba y mantenía los perfiles de usuarios que definen el nivel de acceso a la información autorizada.

Estas tareas también eran realizadas por alguno de los tres operadores de computadoras cuando el Supervisor de Operador de Equipos Electrónicos de Información no estaba en la División de Tecnología.

Las tareas de administración realizadas por dichos empleados resultaban conflictivas e incompatibles con las que efectuaban como parte de los deberes de sus puestos. Esta situación se agravaba al no existir un control alterno de supervisión por parte del Director del NTC sobre las tareas realizadas por estos empleados.

Una situación similar fue comentada en el *Informe de Auditoría TI-03-02* del 29 de octubre de 2002.

Criterio

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 Oficina de Gerencia y Presupuesto (OGP). En esta se establece que las agencias deberán implantar controles adecuados en sus sistemas computadorizados de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Conforme a dicha política y como norma de sana administración, es necesario que se segreguen las funciones relacionadas con las operaciones de los sistemas de información de la entidad, o se establezca la supervisión de las que resultan conflictivas, como control compensatorio. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades y que no se detecten a tiempo.

Efecto

La situación comentada propicia que se incurra en errores o irregularidades y que estos no se puedan detectar con prontitud, con los consiguientes efectos adversos para la entidad.

Causa

Esta situación se debía a que el puesto de Administrador de Seguridad se encontraba vacante, y el Director del NTC no había tomado en consideración el conflicto en las funciones relacionadas con este puesto, realizadas por el Supervisor de Operador de Equipos Electrónicos de Información y los operadores de computadoras.

Comentarios de la Gerencia

En la carta del Superintendente, este nos indicó, entre otras cosas, lo siguiente:

> […] debido a la falta de personal ocasionado por la Ley 7 y Ley 70, en aquel entonces y al presente nos hemos visto en la necesidad de usar los servicios del Supervisor de Operador de Equipos Electrónicos de Información para que asuma el rol de Administrador de Seguridad, Administrador de Sistemas y otras funciones administrativas de dirección, para poder garantizar las operaciones de tecnología y que los servicios de la agencia no se afecten. Se está evaluando la posibilidad de contratar un Administrador de Seguridad luego que termine la Ley 66. [*sic*]

Véase la Recomendación 3.a.

Hallazgo 2 - Deficiencias relacionadas con los controles ambientales y físicos en las áreas en las que se mantenían los equipos de comunicación

Situaciones

a. La Policía contaba con 16 redes virtuales de área y 1 red de área amplia, para la comunicación de sus 139 redes de área local. Los equipos de comunicación correspondientes a estas redes se mantenían en 139 áreas localizadas en el CUJC, las 13 comandancias de área, los 36 precintos[7], los 59 distritos[8], y

[7] Cuarteles de la Policía localizados en el mismo pueblo donde se ubica la Comandancia.

[8] Cuarteles de la Policía localizados en diferentes pueblos, y que están subordinados a una Comandancia.

las 30 unidades especiales[9] de la Policía. En estas áreas se habían instalado gabinetes y estantes para mantener y proteger dichos equipos de comunicación.

El Área de Operaciones Centros de Cómputos de la División de Tecnología era responsable del funcionamiento y del mantenimiento de las redes de comunicación. La misma recibía apoyo técnico del Área de Infraestructura de dicha división y de los coordinadores de Servicios de Tecnología y de los Auxiliares[10], que eran agentes con conocimientos técnicos designados por el Comandante de cada una de las comandancias de área.

El examen efectuado entre el 13 de agosto y el 7 de noviembre de 2013 de los controles ambientales y físicos existentes en 11 de las 139 áreas en las que se mantenían los equipos de comunicación, reveló que no existían las condiciones de seguridad para proteger los sistemas de información computadorizados de la Policía, según se indica:

1) Relacionado con los controles ambientales:

   a) En 7 áreas (64%), se almacenaban cajas de cartón, cables, equipos de telefonía y de computadoras, bombillas, escobas, bolsas plásticas y rollos de papel.

   b) En siete áreas, los equipos de comunicación tenían polvo acumulado.

   c) En 3 áreas (27%), no había equipos para controlar y mantener una temperatura adecuada para los equipos de comunicación. En 1 área (9%), la consola del acondicionador de aire estaba dañada; en 1 la consola estaba en trámites de limpieza; y en la otra no contaban con una consola de acondicionador de aire.

---

[9] Las unidades especiales incluyen unidades o divisiones de tareas especializadas como las divisiones de vehículos hurtados, drogas y vicios, y patrullas de tránsito, entre otras; y las unidades motorizadas, de ciclismo, marítimas y de operaciones especiales. Las unidades especiales responden a las comandancias de área, pero no todas las comandancias cuentan con las mismas unidades.

[10] Estos puestos no estaban establecidos en el *Plan de Clasificación* de la Policía.

d) En 2 áreas (18%), no había extintores de incendio localizados cerca de estas. Además, en 2 áreas los extintores de incendio que estaban cerca de las mismas tenían vencida su fecha de inspección por 7 y 16 meses, y en 1 área el extintor no contaba con la tarjeta de inspección para poder determinar la vigencia de su inspección.

e) En dos áreas, se observaron manchas de humedad en las paredes.

f) En 1 área, los equipos de comunicación no estaban conectados a un generador de energía ininterrumpible (UPS, por sus siglas en inglés); en 2 áreas, el UPS se encontraba dañado; y en 6 áreas (55%), el UPS sólo se utilizaba como protector de sobre carga de voltaje.

g) En un área, el receptáculo de la luz del cuarto donde se ubicaban los equipos no contaba con un interruptor de corriente, lo que no permitía apagar la luz y podía ocasionar un corto circuito.

2) Relacionado con los controles físicos:

a) En siete áreas, el cableado que se conectaba a los equipos de comunicación no estaba organizado ni identificado. Esto era necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones.

b) En siete áreas, el panel con los cables del servicio telefónico se encontraba junto al panel del cableado de la red.

c) En tres áreas, el control de acceso físico no era adecuado. Al momento del examen, las puertas de las áreas se encontraban abiertas.

d) En dos áreas, los equipos de comunicación no estaban instalados dentro de un gabinete o estante, sino que estaban sobre un pedazo de panel, apilados uno encima del otro.

e) En las 11 áreas visitadas, en las que se mantenían los equipos de comunicación, no había un diagrama esquemático que ilustrara las conexiones establecidas entre los *drops*[11] horizontales con los equipos.

Situaciones similares a las del **apartado a.2)c) y e)** fueron comentadas en el *Informe de Auditoría TI-03-13* del 23 de mayo de 2003.

Criterios

Las situaciones comentadas en el **apartado a.1) y 2) de la b) a la e)** son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77*-05. En esta se establece que cada agencia será responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de sus ambientes de tecnología, particularmente sus sistemas críticos. Esto implica que, como norma de sana administración, las agencias deberán tener los cuidados necesarios para proteger los equipos computadorizados contra daños y averías, y para mantener el funcionamiento óptimo de los mismos. Para garantizar razonablemente la seguridad de los equipos y de los sistemas computadorizados, es necesario que:

- Se mantengan los equipos de comunicación en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas. **[Apartado a.1) del a) al c), e) y g), y 2)d)]**
- Se utilice equipo y tecnología adecuada para proteger los sistemas. **[Apartado a.1)d) y f)]**
- Se mantenga organizado e identificado adecuadamente el cableado que conecta los equipos de comunicación de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada. **[Apartado a.2)a)]**
- Se controle adecuadamente el acceso a las áreas donde están ubicados los equipos de comunicación. **[Apartado a.2)b) y c)]**

[11] Es una conexión generalmente utilizada en la red de área local. Son tomas en la pared con una conexión de Ethernet mediante el cual se puede conectar una computadora u otro dispositivo de red.

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada. **[Apartado a.2)e)]**

Además, las situaciones comentadas en el **apartado a.2)a) y e)** son contrarias a lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 77-05*. En esta se establece que las agencias tendrán la responsabilidad de adquirir e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. También se establece que las redes en las agencias deben proveer la infraestructura necesaria para implantar y mantener los procesos de negocio de la agencia, y ser operacionales y confiables.

Efectos

Las situaciones comentadas en el **apartado a.1) y 2)d)** pudieron ocasionar daños y deterioros prematuros a los equipos de la red y a los de computadoras, lo que podría impedir el obtener el rendimiento máximo en términos de los servicios que estos ofrecen.

Las situaciones comentadas en los **apartados a.2)a) y e)** le impiden a la Policía obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Las situaciones comentadas en el **apartado a.2)b) y c)** pudieran propiciar que personas ajenas a las operaciones de la red tengan acceso a los equipos de comunicación. Esto podría representar un riesgo para la continuidad y la disponibilidad de los servicios que ofrece la Policía, así como para la confidencialidad de la información. Además, podrían ocasionar daños a los equipos de comunicación y dificultar el fijar responsabilidades.

Causa

Las situaciones comentadas obedecen a que el Supervisor de Operador de Equipos Electrónicos de Información no había establecido controles de seguridad ambientales y físicos adecuados para proteger los equipos de comunicación de la Policía y sus respectivas conexiones.

Comentarios de la Gerencia

En la carta del Superintendente, este nos indicó, entre otras cosas, lo siguiente:

> Para poder subsanar esta deficiencia, debo contar con el análisis de riesgo el cual me identificara cuales son las debilidades o vulnerabilidades de mi infraestructura tecnológica, ambientales y físicas para así desarrollar un plan de trabajo para corregir todos los puntos mencionados en el hallazgo. Ya se está trabajando la requisición para solicitar el servicio de un análisis de riesgo […]. [*sic*]

Véase la Recomendación 3.b.

Hallazgo 3 - Falta de actualización del diagrama físico de la infraestructura de la red de comunicación de la Policía

Situación

a. Al 12 de septiembre de 2013, la Policía contaba con un diagrama físico de la infraestructura o diseño de la red de comunicación que incluía las redes de área local de las 13 comandancias. Sin embargo, este diagrama no incluía el detalle de las conexiones y de los equipos de comunicación de las restantes 126 redes de área local existentes en el CUJC, los 36 cuarteles de precintos, los 59 cuarteles de distritos y las 30 unidades de servicios especiales.

   Una situación similar fue comentada en el *Informe de Auditoría TI-03-13.*

Criterio

La situación comentada es contraria a lo establecido en la *Política TIG-011* de la *Carta Circular 77-05*. En esta se establece que las agencias deben adquirir e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la

comunicación necesaria para la distribución de servicios eficientemente. Además, incluye como política que el diseño de la red debe estar documentado con diagramas esquemáticos de las redes.

Efectos

La situación comentada impide a la Policía obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Causas

La situación comentada se debía, en parte, a que el Director del NTC no había impartido instrucciones para que el Supervisor de Operador de Equipos Electrónicos de Información preparara un diagrama de las redes de la Policía donde se representaran todas las interconexiones internas y externas de los equipos que componen las mismas. Además, la Policía no contaba con normas y procedimientos escritos para reglamentar el proceso de instalación y de configuración de la red de comunicación.

Comentarios de la Gerencia

En la carta del Superintendente, este nos indicó, entre otras cosas, lo siguiente:

> […] se está trabajando una requisición para la adquisición de los servicios de una compañía para que realice un análisis de toda la red de la policía para los diagramas que mencionan en el hallazgo y de igual forma se documenten. [*sic*]

Véase la Recomendación 3.c. y d.1).

Hallazgo 4 - Falta de activación de la política de contraseñas para requerir que estas fueran combinaciones alfanuméricas, y cuentas de usuarios para acceder a la red con contraseñas expiradas

Situaciones

a. El examen efectuado el 22 de mayo de 2013 sobre los parámetros relacionados con las políticas de auditoría definidos en el sistema operativo del servidor principal de la Policía reveló que no se había

definido la política de contraseñas para requerir que las utilizadas fueran combinaciones alfanuméricas *(Password must meet complexity requirements)*.

b. El examen realizado el 18 de junio de 2013 al servidor principal reveló que de las 3,820 cuentas de usuarios creadas para acceder a la red, 743 (19%) tenían sus contraseñas expiradas. Al considerar los 50 días establecidos en la política del servidor principal para cambiar las contraseñas *(Maximum Password Age)*, determinamos que habían transcurrido entre 28 y 2,517 días luego de la expiración de las mismas.

   Una situación similar a la del **apartado a.** fue comentada en el *Informe de Auditoría TI-03-13.*

Criterio

Las situaciones comentadas son contrarias 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 implantar 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 el uso de las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos; y la verificación periódica de las cuentas con contraseñas expiradas, para determinar si las mismas deben ser eliminadas.

Efectos

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta. Además, propician 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.

Causas

La situación comentada en el **apartado a.** se debía a que el Supervisor de Operador de Equipos Electrónicos de Información, quien tenía a su cargo las funciones del Administrador de Seguridad, no se aseguró de definir la política de contraseñas en el sistema operativo del servidor principal, para que cumpliera con lo establecido en el Artículo II.d de la Sección D. de la *Orden General 2003-25, Normas y Controles para el uso de los Sistemas Computadorizados en la Policía de Puerto Rico*, aprobada el 12 de diciembre de 2003 por el Superintendente.

Lo comentado en el **apartado b.** se debía, en parte, a que el Supervisor de Operador de Equipos Electrónicos de Información tenía a su cargo múltiples tareas, por lo que se le dificultaba realizar el análisis y el mantenimiento periódico de las cuentas de acceso cuyas contraseñas estaban expiradas.

Comentarios de la Gerencia

En la carta del Superintendente, este nos indicó, entre otras cosas, lo siguiente:

> […] se está analizando lo que se requiere para implantar esta política de credenciales. La misma está relacionada con el análisis de riesgo que se está solicitando, el cual es necesario para cumplir con esta política de seguridad. Ya se está trabajando la requisición para solicitar el servicio de un análisis de riesgo. [*sic*]

Véase la Recomendación 3.d.2) y e.

Hallazgo 5 - Falta de un registro del seguimiento, la documentación, el análisis y la solución de los incidentes que ocurren en las redes de los sistemas de información

Situación

a. La OGP mantenía un contrato con una compañía para manejar y examinar continuamente los dispositivos de seguridad de la Oficina del Oficial Principal Ejecutivo de Informática, y de las otras agencias gubernamentales que esta designara. Entre las agencias incluidas en el contrato se encontraba la Policía.

La compañía tenía instalado en el Centro de Cómputos de la Policía un servidor que servía de *firewall*[12], y como mecanismo de detección y prevención de intrusos (IDS/IPS por sus siglas en inglés). Una vez se detectaba una anomalía o incidente de seguridad, la compañía le enviaba un correo electrónico al Supervisor de Operador de Equipos Electrónicos de Información, para que investigara las causas de las anomalías informadas y corrigiera las situaciones.

Al 12 de septiembre de 2013, en la División de Tecnología no se mantenía un registro del seguimiento, la documentación, el análisis y la solución de las anomalías e incidentes de seguridad detectados en los sistemas de información, para en caso de que se repitieran pudiera hacerse referencia a la solución dada a los mismos.

Criterios

La situación comentada es contraria a lo establecido en el Artículo XIV de la Sección D de la *Orden General 2003-25*. En esta se establece que para que la red de telecomunicaciones funcione aceptablemente, es necesario mantener controles adecuados sobre el uso que se les ofrece a sus equipos. El Director del NTC deberá mantener documentación (en forma de *log* o diario) de todos los cambios, los problemas, los servicios, los mantenimientos, las pruebas, las modificaciones en programación, y las violaciones y atentados a la seguridad de los sistemas.

Además, 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 implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Además, deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluidos los límites para esos incidentes en términos de tiempo máximo y tiempo mínimo de respuesta. En consonancia con esto, para garantizar la confiabilidad, la integridad y la disponibilidad de los

[12] Sistema que se coloca entre una red de comunicaciones e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad y autentificación, entre otros.

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.

Efecto

La situación comentada priva a la División de Tecnología de las herramientas y los mecanismos necesarios para identificar las debilidades existentes en la seguridad de los sistemas de información. Además, le impide tener un control eficaz y documentado sobre el manejo de los incidentes ocurridos, con el objetivo de que se puedan tomar las medidas para minimizar sus efectos y prevenir su reincidencia.

Causa

La situación comentada se atribuye a que el Director del NTC no había impartido instrucciones para que el Supervisor de Operador de Equipos Electrónicos de Información mantuviera un registro relacionado con la documentación del análisis de los incidentes que ocurren en las redes de los sistemas de información.

Comentarios de la Gerencia

En la carta del Superintendente, este nos indicó, entre otras cosas, lo siguiente:

> […] se está trabajando con un plan para analizar los logs de los sistemas de seguridad como FireEye y Forti Analizer. Para desarrollar un registro de seguimiento, documentación, análisis de anomalías y solución de las mismas. Se comenzó con el analices de unos logos preliminarmente y se identificaron computadoras infectadas y se trabajó unas acciones correctivas. [*sic*]

Véase la Recomendación 3.d.3).

COMENTARIO ESPECIAL

En esta sección se comentan situaciones que no necesariamente implican violaciones de leyes y de reglamentos, pero que son significativas para las operaciones de la entidad auditada. También se incluyen situaciones que no están directamente relacionadas con las operaciones de la entidad, las cuales pueden constituir violaciones de leyes o de reglamentos, que afectan al erario.

Inversión millonaria de fondos públicos en la implantación de proyectos de tecnología para computadorizar las patrullas de la Policía, sin lograr los objetivos

Situación

a. Entre mayo de 1992 y junio de 2012, se iniciaron tres proyectos, a cargo de distintas entidades gubernamentales, para proveerles equipos tecnológicos a las patrullas de la Policía. Esto, con el objetivo de que estas patrullas se pudieran comunicar con distintas bases de datos para obtener información sobre conductores, licencias y vehículos de motor.

   Estos proyectos fueron descontinuados sin que la Policía hubiera logrado obtener beneficios de la inversión realizada en los mismos, según se indica:

   1) El 18 de mayo de 1992 se creó la Junta Operacional para Acción Vehicular (JOAV), mediante el *Boletín Administrativo OE-1992-32*, *Orden Ejecutiva del Gobernador del Estado Libre Asociado de Puerto Rico para crear la Junta Operacional para Acción Vehicular y Asignarle Facultades y Deberes.* La JOAV estaba compuesta por el Director Ejecutivo de la Administración de Compensaciones por Accidentes de Automóviles (ACAA), quien sería el Presidente; el Secretario de Transportación y Obras Públicas; y el Superintendente de la Policía. La misma tenía la responsabilidad de dirigir y de coordinar la implantación y la utilización de las tecnologías de informática y comunicaciones para controlar las actividades delictivas y los accidentes que involucraran automóviles. Este proyecto se conoció como Proyecto Interagencial de Acción Vehicular (PIAV), y sus objetivos eran, entre otros, obtener mediante unos terminales de computadoras información sobre las vigencias de las licencias de conducir, de los antecedentes del conductor en cuanto a los accidentes de tránsito y el uso de alcohol o drogas, y de los vehículos hurtados y su uso en actos delictivos; y reducir el tiempo en que las patrullas de la Policía y las unidades de emergencias médicas llegaban a prestar servicios en lugares de accidentes

de tránsito. Como parte de los esfuerzos para el desarrollo del PIAV, entre agosto y diciembre de 1992 la ACAA invirtió $21.7 millones, de los cuales $13.7 millones fueron utilizados para la adquisición de equipos de computadoras y servicios para la Policía.

En 1993, el PIAV fue descontinuado por el Director Ejecutivo de la ACAA por entender que el mismo no respondía a los mejores intereses de esta. Esto sin haberse logrado los objetivos trazados en dicho proyecto. El equipo adquirido para la Policía fue transferido a esta y utilizado para otros propósitos.

Los detalles de este proyecto se comentaron en el *Informe de Auditoría CPED-96-11* del 30 de junio de 1996.

2) En febrero de 1999, la Policía inició un proyecto, que se conoció como el *Sistema de Automatización de Patrullas*[13], para proveer comunicación inalámbrica entre el Cuartel General y las patrullas. Para esto, designó un Comité Evaluador con el objetivo de investigar y evaluar la tecnología y las compañías disponibles en el mercado. El 16 de julio de 1999 el Superintendente de la Policía otorgó el Contrato 040001007 a una compañía por $6.3 millones para la implantación y la integración de dicho sistema. Entre el 22 de septiembre de 2000 y el 4 de mayo de 2001, la Policía adquirió 250 computadoras y 250 impresoras portátiles para instalarlas en las patrullas.

   Luego de haberse adquirido este equipo de dos compañías a un costo de $3.1 millones, y de haberle pagado $1.7 millones a la compañía que realizaría la implantación y la integración del sistema, esta última incumplió con el contrato al declararse en quiebra, por lo que el proyecto no se completó. El equipo adquirido se mantenía almacenado sin uso alguno.

[13] Este sistema se conoció posteriormente como LERS *(Law Enforcement Records System).*

Los detalles de este proyecto se comentaron en el *Informe de Auditoría TI-04-06* del 12 de abril de 2004.

3) El 10 de junio de 2011 el Gobernador de Puerto Rico aprobó la *Resolución Conjunta 54* para autorizar a la OGP a utilizar $610 millones provenientes del *Fondo de Estímulo Económico de Puerto Rico* creado mediante la *Ley 1-2009*, según enmendada. Mediante dicha *Resolución*, se asignaron $20.3 millones para el pago de Proyectos de Tecnologías de Información Gubernamental. El 28 de junio de 2012 se formalizó el *Acuerdo de Entendimiento y Cooperación Interagencial 2012-BGF-151 (Acuerdo)* entre la Policía; los departamentos de Transportación y Obras Públicas, de Hacienda, de Justicia y del Trabajo y Recursos Humanos; las autoridades de Carreteras y Transportación de Puerto Rico, de Edificios Públicos, y de Energía Eléctrica de Puerto Rico; la OGP; y el Banco Gubernamental de Fomento para Puerto Rico (BGF). Esto, para coordinar esfuerzos, aplicar las respectivas pericias administrativas en conjunto, y cooperar para la ejecución de los proyectos de tecnología para la seguridad pública, que consistirían en la implantación de:

   - Un sistema de terminales de data móviles (tabletas) y multas electrónicas
   - Un sistema de vídeo vigilancia, cuyo alcance abarcaría la División de Patrullas de Autopista de Salinas, y varias secciones del Expreso Baldorioty de Castro y del Túnel Minillas.

   En el Acuerdo se incluyeron las responsabilidades de cada agencia relacionadas con el sistema de terminales de data móviles y multas electrónicas, según se indica:

   - El BGF sería la entidad contratante en la formalización de los contratos necesarios para la viabilidad de los proyectos de tecnología para la seguridad pública en todos sus aspectos.

- La OGP estaría encargada de identificar y de transferir los fondos para el cumplimiento de los proyectos de este Acuerdo.
- La Policía y la Autoridad de Carreteras y Transportación de Puerto Rico permitirían al personal contratado el acceso a las instalaciones del cuartel y a las patrullas de la División de Patrullas de Autopista de Salinas, y a cualquier otra unidad que participara en el sistema de terminales de data móviles, para instalar y proveer mantenimiento a las aplicaciones y a los equipos necesarios para el funcionamiento del proyecto.
- El Departamento de Transportación y Obras Públicas (DTOP) se encargaría de que sus sistemas y bases de datos contaran con los mecanismos de integración necesarios para que los terminales de data móviles pudieran leer los datos y la información allí almacenada, y que desde estos se pudieran registrar nuevos datos e información. El acceso provisto mediante los terminales debería cumplir con los parámetros de confidencialidad y de seguridad establecidos por las leyes estatales y federales aplicables, según implementadas por el DTOP.
- El Departamento de Justicia se encargaría de supervisar al personal contratado para trabajar en las actualizaciones y en los cambios necesarios para que el *Criminal Justice Information System* (CJIS) fuera operacional y estuviera vigente al momento de ejecutar los proyectos, y se aseguraría de que su sistema *Récord Criminal Integrado* (RCI) funcionara adecuadamente para que se pudiera extraer la información necesaria para proveer alertas de posibles amenazas a los policías en todo momento. Además, permitiría a los proveedores acceder a sus instalaciones para que integraran el sistema de terminales de data móviles al CJIS y al RCI. Esto, sujeto a que el Departamento de Justicia cumpliera con las obligaciones que por reglamentación federal

se le exigen; proveería los ambientes de prueba y producción necesarios para el funcionamiento del sistema; y daría acceso a los administradores de dicho sistema, sujeto a las políticas de seguridad establecidas para el proyecto.

- El Departamento de Hacienda proveería cuentas de acceso en ambientes de prueba y de producción para procesar los pagos realizados por los ciudadanos en los terminales de data móviles, a través del servicio web de la Colecturía Virtual que se ofrece mediante el Portal Oficial del Estado Libre Asociado de Puerto Rico.

Los proyectos serían sufragados con fondos identificados por la OGP para la implantación de los mismos. La totalidad de los fondos serían transferidos al BGF, para ser depositados en una cuenta separada para esos efectos.

El 13 de julio de 2012 el BGF otorgó el Contrato 2013-BGF046 con una compañía para la implantación del proyecto piloto *Mobile Data Terminals and Electronic Ticket System* en la División de Patrullas de Autopista de Salinas. Este proyecto tenía como objetivos optimizar el proceso de emisión de multas, mediante la utilización de terminales de data móviles, y generar alertas provenientes de varios sistemas de agencias de seguridad, para permitir que el agente estuviera mejor informado al momento de intervenir en cualquier situación. El contrato tenía vigencia del 13 de julio de 2012 al 15 de septiembre de 2013, y un costo de $429,410 que incluía: $175,960 para la adquisición de 20 terminales de data móviles (tabletas) y servicios de conexión de datos *(Data Airtime)*, $24,450 para la adquisición de la aplicación y el servicio de Internet para conectarse al Sistema DAVID Plus, y $229,000 para servicios profesionales.

El proyecto, además, proveía para recibir alertas de seguridad de varios sistemas como el *National Crime Information Center* (NCIC), que provee alertas sobre antecedentes penales y vehículos

hurtados; el RCI, que provee alertas sobre ofensores sexuales; y el Sistema DAVID Plus, que provee alertas sobre vehículos hurtados y desaparecidos, multas pendientes de pago, y la información del conductor y el vehículo.

El 30 de octubre de 2012 el contrato se enmendó (Contrato 2013-BGF046-A), por $281,652[14] para:

- Dividir el proyecto en dos fases. La fase I requería equipos y materiales adicionales para implantar la aplicación en la División de Patrullas de Autopista de Salinas. Luego en la fase II se determinaría la cantidad de terminales de data móviles, equipos, materiales y servicios necesarios para apoyar la misma.

- Cambiar la cantidad y el tipo de terminales de data móviles a implantar en la fase I de 20 marca Panasonic[15] a 8 marca Samsung, e instalar una aplicación distinta a la indicada en el contrato original.

El proyecto piloto se implantó en las divisiones de Patrullas de Autopista de Salinas y de Carreteras de Aguadilla por un total de $354,650[16]. En Salinas los trabajos relacionados con el proyecto se realizaron desde julio hasta septiembre de 2012, y se distribuyeron 11 tabletas: 8 (fase I) se asignaron a patrullas equipadas y 3 (fase II) a la estación de pesaje. En Aguadilla los trabajos se realizaron desde octubre hasta diciembre de 2012, y se asignaron 14 tabletas (fase II) a patrullas equipadas.

El 13 de junio de 2013 el Vicepresidente y Agente Fiscal del BGF le envió una carta a la compañía contratada para informarle que el BGF había decido rescindir el contrato, efectivo 30 días luego de

[14] De estos, $28,202 eran para la adquisición de equipos (8 tabletas) y servicios de *Data Airtime Plan*, $24,450 para la adquisición del programa y servicio web para la conexión al Sistema DAVID Plus, y $229,000 para servicios profesionales.

[15] Los equipos y materiales necesarios para la Fase II se determinarían luego de completada la Fase I.

[16] El último pago se realizó el 7 de agosto de 2013.

la fecha de recibo de dicha carta. La razón por la que se rescindió el contrato fue porque la Policía le informó al BGF que las tabletas adquiridas bajo este contrato no se utilizaban debido a que no estaban conectadas al sistema de información del Departamento de Justicia. Esto, por la preocupación de que las mismas comprometieran la seguridad de dicho Departamento. Las 25 tabletas fueron utilizadas desde septiembre hasta noviembre de 2012, y fueron removidas de las divisiones de Patrullas de Autopista de Salinas y de Carreteras de Aguadilla el 16 de agosto de 2013. Las mismas se mantenían almacenadas en el Cuartel General de la Policía sin darles uso alguno.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Ley Núm. 230*. En esta se establece, como política pública, que los gastos del Gobierno se harán dentro de un marco de utilidad y austeridad. Es responsabilidad de la gerencia de toda entidad gubernamental garantizar la inversión de los fondos y la utilización efectiva de los recursos disponibles. Esto implica que, como norma de sana administración, la inversión de fondos públicos para la implantación de sistemas computadorizados debe planificarse, de manera que se obtengan los beneficios esperados en un tiempo razonable.

Efectos

Las situaciones comentadas no permitieron que la Policía obtuviera el beneficio esperado de los $18.9 millones invertidos. Luego de transcurridos más de 20 años desde el inicio del primer proyecto, las patrullas de la Policía aún no cuentan con el equipo tecnológico que le permita a sus agentes acceder a los sistemas, y a las bases de datos de seguridad pública y del Sistema DAVID Plus, al momento de realizar las intervenciones, y obtener información en tiempo real *(real time)* sobre las personas y los vehículos intervenidos. Dicha información sería de gran utilidad para el cumplimiento de la misión de proteger a las personas y a la propiedad, y de mejorar la calidad de vida en Puerto Rico; y para proteger las vidas de los agentes.

Actualmente, las patrullas sólo cuentan con unidades de comunicación de radio frecuencia (radio móvil)[17] mediante las cuales los agentes se comunican con el Centro de Mando de la Policía, en donde se les provee la información sobre las personas y los vehículos intervenidos.

Además, la Policía aún no cuenta con un sistema para emitir electrónicamente los boletos de multa por violaciones a la *Ley de Tránsito*, el cual apoyaría los procesos de registro, por parte del DTOP, y de cobro, por parte del Departamento de Hacienda, de los mismos.

Causas

La situación se debe principalmente a la falta de una planificación adecuada para establecer los distintos proyectos que considerara, entre otras cosas, el costo-beneficio de estos, la solidez económica de las compañías contratadas, la infraestructura adecuada y necesaria para dar apoyo a los equipos adquiridos, y la seguridad y la protección de la información de las bases de datos que sería compartida.

Además, lo comentado en el **apartado a.3)** se atribuye a que desde la etapa de implantación del proyecto, el Secretario de Justicia no se aseguró de que se consideraran las medidas de seguridad requeridas por el Gobierno Federal, relacionadas con el uso de equipo móvil, y con el acceso al CJIS y al RCI.

Véanse las recomendaciones 1, 2 y 4.

RECOMENDACIONES

Al Gobernador del Estado Libre Asociado de Puerto Rico

1. Ver que para futuros proyectos de tecnología para la seguridad pública, en los que se integren recursos de distintas entidades gubernamentales, se coordinen y se supervisen adecuadamente las tareas asignadas a cada entidad. Esto, de manera que se asegure el cumplimiento de los objetivos y el beneficio esperado de la inversión realizada en dichos proyectos. **[Comentario Especial]**

[17] Si la patrulla no cuenta con un radio móvil, a los agentes se les proveen radios portátiles para esta comunicación.

Al Secretario de Justicia

2. Ver que para futuros proyectos de tecnología para la seguridad pública, en los que sea necesario proveer acceso a la información de las bases de datos de los sistemas de información, tales como: el CJIS y el RCI, se consideren las medidas de seguridad requeridas por el Gobierno Federal para asegurar la protección de la misma. **[Comentario Especial]**

Al Superintendente de la Policía

3. Ejercer una supervisión eficaz sobre el Superintendente Auxiliar de Servicios Gerenciales para asegurarse de que el Director del NTC:

    a. Establezca los controles necesarios para que se mantenga una segregación adecuada de las funciones conflictivas que realizan el Supervisor de Operador de Equipos Electrónicos de Información y los operadores de Computadoras, relacionadas con la asignación, la activación y la eliminación de cuentas de acceso, y la creación y el mantenimiento de perfiles de usuarios. De no ser posible mantener dicha segregación, establezca controles alternos de supervisión y de revisión sobre las actividades que realizan estos empleados. **[Hallazgo 1]**

    b. Establezca, junto con los coordinadores de Servicios de Tecnología de las comandancias, los controles necesarios para corregir las situaciones indicadas en el **Hallazgo 2**. Esto, de manera que se asegure de que los equipos de comunicación de la Policía se mantengan en lugares donde estén debidamente protegidos contra accesos no autorizados y contra posibles daños causados por condiciones ambientales y físicas, que puedan afectar la confidencialidad de la información, y la disponibilidad y el rendimiento de estos equipos.

    c. Redacte normas y procedimientos para reglamentar el proceso de instalación y de configuración de la red. Como parte de estos, se

debe requerir que se actualicen periódicamente los diagramas físicos de la infraestructura de la red de comunicaciones de la Policía. **[Hallazgo 3]**

d. Instruya al Supervisor de Operador de Equipos Electrónicos de Información para que:

1) Actualice el diagrama físico de la infraestructura de las redes de la Policía para que incluya las correspondientes a todos los precintos, los distritos, el CUJC y las unidades especiales. **[Hallazgo 3]**

2) Modifique el parámetro de seguridad del sistema operativo del servidor principal para requerir que las contraseñas tengan una combinación de caracteres alfanuméricos (letras, símbolos y números), según se establece en la *Orden General 2003-25*. **[Hallazgo 4-a.]**

3) Prepare un registro o bitácora en la que se documente el análisis, el seguimiento y la solución de las anomalías e incidentes de seguridad que se detectan en los sistemas de información. **[Hallazgo 5]**

e. Evalúe las tareas asignadas al Supervisor de Operador de Equipos Electrónicos de Información y determine si es necesario asignar algún otro empleado, de manera que pueda asegurarse el análisis y el mantenimiento periódico de las cuentas de acceso con contraseñas expiradas. Esto, con el propósito de identificar cuáles de estas no son necesarias para las operaciones de la Policía y sus sistemas de información, y evaluar la eliminación de las mismas. **[Hallazgo 4-b.]**

4. Ver que para futuros proyectos relacionados con los sistemas de información se preparen estudios de necesidad y de viabilidad. Estos permitirán, entre otras cosas, realizar una planificación adecuada en la que se consideren los objetivos; la infraestructura tecnológica, el personal y los fondos necesarios; el costo-beneficio del proyecto; y la seguridad y la protección de la información de las bases de datos que

serán compartidas. Además, ver que se planifique y se supervise de forma adecuada la contratación de los servicios relacionados con dichos proyectos, para que se logren eficazmente sus objetivos, se obtengan los beneficios esperados y se maximice el uso de la inversión realizada. **[Comentario Especial]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yasmín M. Calaf

ANEJO 1

POLICÍA DE PUERTO RICO
NEGOCIADO DE TECNOLOGÍA Y COMUNICACIONES
DIVISIÓN DE TECNOLOGÍA
INFORME PUBLICADO

INFORME	FECHA	CONTENIDO DEL INFORME
TI-15-01	14 oct. 14	Resultado del examen de los controles internos establecidos para la administración del programa de seguridad y la continuidad del servicio.

ANEJO 2

POLICÍA DE PUERTO RICO
NEGOCIADO DE TECNOLOGÍA Y COMUNICACIONES
DIVISIÓN DE TECNOLOGÍA
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. James Tuller Cintrón	Principal Oficial de Seguridad Pública y Superintendente Designado	1 dic. 13	20 dic. 13
Sr. Héctor M. Pesquera López	Superintendente	8 oct. 12	15 nov. 13
Vacante	Superintendente Asociado	16 nov. 13	20 dic. 13
Sr. Ricardo Martínez Rodríguez	"	4 dic. 12	15 nov. 13
Sr. José L. Rivera Díaz	"	8 oct. 12	30 nov. 12
Sra. Yasmín González Morales	Superintendente Auxiliar en Servicios Administrativos	11 feb. 13	20 dic. 13
Sr. Ángel Cortés Cintrón	"	8 oct. 12	31 ene. 13
Sr. Luis González Sánchez	Director del Negociado de Tecnología y Comunicaciones[18]	13 feb. 13	20 dic. 13
"	"	8 oct. 12	15 dic. 12
Vacante	Director de la División de Tecnología[19]	8 oct. 12	20 dic. 13

[18] Este puesto estuvo vacante durante el período del 16 de diciembre de 2012 al 12 de febrero de 2013.

[19] El Tte. Julio De Jesús Rivera realizó las tareas de este puesto del 8 de octubre al 7 de diciembre de 2012. A partir del 13 de diciembre de 2012, dichas tareas fueron asignadas al Sr. Caonabo Vicente Vázquez, Supervisor de Operador de Equipos Electrónicos de Información.

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