INFORME DE EXAMEN

OIG-E-24-003

Oficina del Inspector General
Gobierno de Puerto Rico

Departamento de Transportación y Obras Públicas

Controles en los accesos otorgados y la seguridad del *Sistema Drivers and Vehicles Information Databases Plus* (David+)

11 de septiembre de 2023

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

El Área de Pre-intervención y Exámenes de la Oficina del Inspector General de Puerto Rico (en adelante, OIG), en su labor preventiva, realizó un examen de cumplimiento sobre los controles de los accesos otorgados y la seguridad del Sistema *Drivers and Vehicles Information Databases Plus* (en adelante, DAVID+), establecidos por el Departamento de Transportación y Obras Públicas (en adelante, DTOP) y la Autoridad de Carreteras y Transportación (en adelante, ACT).

El examen realizado reflejó las siguientes deficiencias:

1. Servidores donde reside el Sistema DAVID+ y equipo de comunicación obsoleto y sin soporte técnico del fabricante.

2. Falta de un Plan Estratégico de Tecnología de Información.

3. Falta de un análisis de riesgos de los sistemas de información computadorizados y un Plan de Seguridad.

4. Deficiencias en el Plan de Contingencias del Área de Tecnología de Información.

5. Falta de un centro alterno para la recuperación de las comunicaciones.

6. Falta de un plan y de un registro para el manejo de incidentes de seguridad.

7. Incumplimiento en someter el nombramiento del Oficial Principal de Informática al *Puerto Rico Innovation and Technology Service* (en adelante, PRITS).

8. Falta de organización de los cables que se conectaban a los equipos de comunicación.

9. Deficiencias relacionadas con la administración de las cuentas de acceso activas a exempleados en el Sistema DAVID+.

10. Falta de controles físicos en el área del servidor donde reside el Sistema DAVID+.

11. Fallas relacionadas con el diagrama esquemático de la red de comunicaciones.

12. Fallas relacionadas con los controles ambientales en el *Minillas Data Center.*

13. Deficiencias relacionadas con el informe de inventario de la Oficina de Sistema de Información (en adelante, OSI) del DTOP y del Área de Tecnología de Información (en adelante, ATI) de la ACT y de los programas instalados en las computadoras.

14. Falta de adiestramientos continuos a los usuarios sobre el uso de los sistemas de información y las políticas de seguridad y otras deficiencias en la implantación de éstas.

15. Reglamentación de los sistemas de información sin actualizar.

Conforme con lo establecido en el Artículo 17 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (Ley Núm. 15-2017), la OIG remite el presente informe a la autoridad nominadora para que tome las medidas correctivas necesarias ante el incumplimiento de procedimientos internos por parte de sus empleados o funcionarios y notifique a la OIG las acciones tomadas para garantizar el fiel cumplimiento de las leyes y reglamentos aplicables.

La OIG está comprometida en fomentar niveles óptimos de integridad, honestidad, transparencia, efectividad y eficiencia en el servicio público. De igual forma rechaza todo acto, conducta o indicio de corrupción por parte de funcionarios o empleados públicos que inflija sobre la credibilidad del Gobierno de Puerto Rico y sus entidades.

De conocer sobre actos que podrían poner en peligro el buen uso de fondos públicos, así como actos que podrían constituir corrupción, puede comunicarse con la línea confidencial de la OIG al 787-679-7979, enviar correo electrónico a informa@oig.pr.gov o vía electrónica a través de www.oig.pr.gov/informa.

El presente informe se hace público conforme con lo establecido en la Ley Núm. 15-2017, según enmendada, y otras normativas aplicables.

INFORMACIÓN DE LA ENTIDAD

La Sección 6 del Artículo IV de la Constitución de Puerto Rico de 25 de julio de 1952, establece el Departamento de Obras Públicas, sin perjuicio de la facultad de la Asamblea Legislativa para crear, reorganizar y consolidar departamentos ejecutivos del Gobierno.

Conforme al Plan de Reorganización Núm. 6 de 1971, según enmendado, el cual entró en vigor el 2 de enero de 1973, se reorganiza para asignarle la responsabilidad como organismo central a cargo del Programa de Transportación del Gobierno de Puerto Rico, y se redenomina el Departamento de Transportación y Obras Públicas. Dicho Plan de Reorganización también adscribe la Autoridad de Carreteras y Transportación, la Autoridad Metropolitana de Autobuses (AMA) y la Autoridad de los Puertos al DTOP. La Ley Núm. 123-2014, según enmendada, conocida como *Ley de la Autoridad de Transporte Integrado de Puerto Rico*, crea la Autoridad de Transporte Integrado de Puerto Rico (ATI) y la adscribe al DTOP.

Mediante la Ley Núm. 33 del 25 de mayo de 1972, según enmendada, se adscribió la Comisión para la Seguridad en el Tránsito. Por virtud de la Ley Núm. 65 del 17 de agosto de 1989, se le concedió autonomía fiscal a la Autoridad de los Puertos y se separó del DTOP. Mediante la Ley 1-1991, se redenominó a la Autoridad de Carreteras como la Autoridad de Carreteras y Transportación (ACT) y se facultó para que fuera la principal responsable del plan de transportación y para implementar la política pública sobre la transportación colectiva establecida por el Secretario de Transportación y Obras Públicas (Secretario). Además, la Ley Núm. 1-2000,

según enmendada, creó la Autoridad de Transporte Marítimo de Puerto Rico y las Islas Municipio adscrita al DTOP.

El DTOP es responsable de implementar la planificación, promoción y coordinación de la actividad gubernamental en el campo de la transportación, y de formular la política pública relacionada con la transportación terrestre, aérea y marítima del Gobierno de Puerto Rico. Además, ofrece exámenes de conductor, hace obligatoria la inspección de los vehículos de motor, regula el uso y la fijación de rótulos en las carreteras, administra la propiedad inmueble del Gobierno, realiza estudios y diseños para el mejoramiento de las carreteras, desarrolla campañas educativas para la prevención de accidentes de tránsito, realiza obras para corregir los daños ocasionados por fenómenos naturales en las carreteras, y conserva, diseña y reconstruye las obras realizadas por el Gobierno, entre otras cosas.

El DTOP es dirigido por un secretario nombrado por el Gobernador con el consejo y consentimiento del Senado de Puerto Rico. Para realizar sus funciones, el DTOP cuenta con las secretarías auxiliares de Administración y Recursos Humanos, y de Planificación, Programación y Control, y por las directorías de Servicios al Conductor, Desarrollo Comunitario, Obras Públicas, y Urbanismo. La Directoría de Obras Públicas cuenta con 7 oficinas regionales localizadas en Aguadilla, Arecibo, Guayama, Humacao, Mayagüez, Ponce y San Juan. La Directoría de Servicios al Conductor (DISCO) está compuesta por 15 centros de servicios al conductor (CESCO) localizados en Aguadilla, Arecibo, Barranquitas, Bayamón, Caguas, Carolina (Metropolitano), Fajardo, Guayama, Humacao, Manatí, Mayagüez, Ponce, Río Piedras, Utuado y Vieques.

La ACT se encuentra dentro de la estructura organizacional del Departamento. Bajo la ACT está el Área de Administración y bajo ésta el ATI, quien se encarga de dar apoyo al DTOP y a la DISCO.

El ATI de la ACT, se encargaba de dar apoyo al DTOP y a la DISCO en cuanto a las operaciones relacionadas con los sistemas de información computadorizados de estos. El ATI tenía cuatro oficinas: Director, Desarrollo y Mantenimiento de Sistemas, Apoyo Técnico y Operaciones.

Entre otras cosas, el ATI de la ACT es responsable de las redes de comunicación de datos del DTOP y de la propia ACT y es el responsable de la administración del Sistema DAVID+. En el Sistema DAVID+ se procesa la información relacionada con los conductores y los vehículos de motor, tal como: la emisión y la renovación de las licencias de conducir y de los permisos de vehículos de motor o arrastres (marbetes). Además, se procesa la información de las multas asociadas a las licencias y los marbetes. El usuario principal de la información contenida en el Sistema DAVID+ es DISCO, pero también la utiliza personal externo, tales como: el ATI, la Policía de Puerto Rico, la Administración de Compensaciones por Accidentes de Automóviles (ACAA), y la Administración para el Sustento de Menores (ASUME), entre otras agencias de ley y orden estatales como federales; y el público en general. El Sistema David+ reside y es mantenido y custodiado fuera del DTOP y la ACT.

BASE LEGAL

El presente informe se emite en virtud de los Artículos 7, 8, 9 y 17 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.

OBJETIVOS

El examen estuvo dirigido a determinar si los controles de los accesos otorgados y la seguridad del sistema DAVID+ se realizaron de acuerdo con las siguientes leyes y normativas aplicables:

1. Ley Núm. 75-2019, según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service* (PRITS).

2. Ley Núm. 230 del 23 de julio de 1974, según enmendada, *Ley de Contabilidad del Gobierno de Puerto Rico.*

3. Ley Núm. 8-2017, según enmendada, conocida como *Ley para la Administración y Transformación de los Recursos Humanos en el Gobierno de Puerto Rico.*

4. Ley Núm. 38-2017, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico.*

5. Reglamento 11 *Normas Básicas para el Control y Contabilidad de los Activos Fijos*, aprobado el 29 de diciembre de 2005, por el secretario del Departamento de Hacienda.

6. *6 CFR2 § 37.41 - Security plan del Real ID Act del 2005 y Attachment A Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the Real ID Act.*

7. *Federal Information System Controls Audit Manual* (FISCAM), promulgado por el *Government Accountability Office* (GAO).

8. Política Núm. ATl-004, *Servicios de Tecnología de la Carta Circular Núm. 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 (en adelante, Carta Núm. 140-16) emitida por la Oficina de Gerencia y Presupuesto (OGP) el 30 de septiembre de 2011, revisada el 12 de octubre de 2016, y administrada por la PRITS.*

9. Política Núm. ATI-008, *Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la Carta Circular Núm. 140-16.

10. Política Núm. ATl-011, *Mejores Prácticas de Infraestructura Tecnológica* de la Carta Circular Núm. 140-16.

11. Política Núm. ATI-015, *Programa de Continuidad Gubernamental* de la Carta Circular Núm. 140-16.

12. La Orden Administrativa PRITS-2021-002, emitida el 12 de abril de 2021, por el Principal Ejecutivo de Innovación e Información del Gobierno y Director Ejecutivo – PRITS.

13. La *Política para la Seguridad Cibernética* y los *Estándares para la Seguridad Cibernética* aprobada el 29 de octubre de 2021, por PRITS.

14. Plan de Contingencia (Plan), revisado al 18 de junio de 2009, por el director ejecutivo de la ACT.

15. Boletín Administrativo Núm. OE-2021-007, *Orden Ejecutiva del gobernador de Puerto Rico, Hon. Pedro R. Pierluisi, para decretar como política pública la aceleración del gobierno digital, el desarrollo de la intercomunicación e interoperabilidad de los sistemas de tecnología del gobierno*, emitido el 4 de enero de 2021.

16. Orden Administrativa Núm. PRITS 2021-003, emitida el 12 de abril de 2021, por la PRITS, sobre *Establecer las directrices sobre nombramiento(s) de oficial(es) principal(es) de informática (OPI) de las agencias bajo la jurisdicción de Puerto Rico Innovation & Technology Service en cumplimiento con la Ley Núm. 75-2019.*

17. Propuesta *Information Technology DTOP, Datacenter Collocation and Virtual Hosting Replication Services, Technical Support Services and Network Monitoring* del 12 de febrero de 2020, la cual forma parte del Contrato entre una compañía privada y el DTOP.

ALCANCE Y METODOLOGÍA

El examen cubrió desde el 1 julio de 2021 al 31 de agosto de 2022.

La metodología utilizada fue la siguiente:

1. Entrevistas a servidores públicos.

2. Inspecciones físicas.

3. Exámenes y análisis de informes y de documentos generados por el DTOP, la ACT y por fuentes externas.

4. Pruebas y análisis de información financiera, de procedimientos de control interno, de confiabilidad de los datos procesados por computadoras y de otros procesos.

5. Validación de información obtenida.

En algunos aspectos, se examinaron transacciones, documentos y operaciones de fechas anteriores y posteriores.

HALLAZGOS

Hallazgo 1 – Servidores donde reside el DAVID+ y equipo de comunicación obsoleto y sin soporte técnico del fabricante

Situación

Las entidades gubernamentales deben desarrollar procedimientos para identificar, informar y responder rápidamente al percatarse de la obsolescencia de los equipos computadorizados. Es política pública del gobierno crear un nuevo andamiaje de gobierno innovador, atemperado a las exigencias del siglo XXI y capaz de valerse de la tecnología avanzada, para cumplir con las expectativas de la ciudadanía y con los estándares modernos de gobernanza efectiva. Esto responde a que está probado que la innovación en los desarrollos tecnológicos y en la programación informática promueve la eficiencia gubernamental y un manejo más apropiado de los recursos humanos y físicos, lo que se traduce en un desarrollo económico de Puerto Rico positivo.

Asimismo, en la evaluación realizada con la información sometida por la OSI del DTOP y el ATI de la ACT; en quien DTOP delegó la administración del sistema DAVID+ sobre los inventarios físico de los equipos computadorizados, reveló que:

a. Los dos (2) servidores donde reside DAVID+ marca IBM Modelo *Power* 570, se encuentran obsoleto y sin apoyo técnico. La IBM retiro el 7 de enero de 2011, los equipos del mercado y descontinuó su soporte técnico el 31 de marzo de 2019[1].

b. Un enrutador (*Router*) Cisco 7606 utilizado para la conexión con la red de una compañía de servicios, la *Puerto Rico Electric Power Authority* (PREPA), la OGP y la retrasmisión con el sitio de la réplica (*Prime Venture Data Center*). A la fecha del examen el enrutador (*Router*) Cisco 7606 se encontraba obsoleto y sin apoyo técnico. Este fue retirado del mercado el 24 de julio de 2016 y no cuenta con soporte técnico del fabricante desde el 31 de julio de 2021[2].

Criterio

Las situaciones comentadas son contrarias con a las siguientes disposiciones:

El Artículo 13. — *Oficial Principal de Informática de las agencias*, apartados (g) y (h) de la Ley Núm. 75-2019, según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service* (PRITS) (en adelante, Ley Núm. 75-2019), que dispone lo siguiente:

[1] Información obtenida de la página electrónica de los fabricantes.

Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, el Oficial Principal de Informática de cada agencia, o en su defecto, el director o directores de información y tecnología de toda agencia, tendrán que cumplir con las políticas, protocolos, guías operacionales dispuestas por el PEII[2] *y los siguientes deberes y responsabilidades:*

(g) Desarrollar, mantener y facilitar la implantación de una estructura segura e integrada de las tecnologías de información y comunicación.

(h) Promover el diseño y la operación eficiente y efectiva de los sistemas de información, incluyendo mejoras a éstos.

La Sección *Política*, Apartado *Procedimiento*, Inciso B *Responsabilidades de la Agencia*, Subinciso 2 *Planificación* (2) de la Política Núm. ATl-004, *Servicios de Tecnología* de la Carta Circular Núm. 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* (en adelante, Carta Núm. 140-16), emitida por la Oficina de Gerencia y Presupuesto (OGP) el 30 de septiembre de 2011, revisada el 12 de octubre de 2016, y administrada por la PRITS, establece que:

Todas las agencias cubiertas por esta política deberán cumplir las normas y procedimientos relativos al uso de las tecnologías de la información que se detallan a continuación. Estas políticas tienen como meta obtener los beneficios de los adelantos en la tecnología, mejorar las relaciones interagenciales y la reducción de costos operacionales.

PROCEDIMIENTO

B. Responsabilidades de la Agencia:

Planificación

2. *La Agencia, coma parte de un* ***proceso de actualización y optimización****, verificará sus sistemas anualmente para identificar posibles modificaciones a los mismos. De esa manera, se garantiza un servicio de alta calidad. Estas verificaciones se utilizarán también en la creación del presupuesto anual de tecnología. [Énfasis nuestro]* (**Ver Hallazgo 2**)

[2]PEII. — Significa el Principal Ejecutivo de Innovación e Información del Gobierno de Puerto Rico.

La Sección *Plataforma* Apartado *Política para el Componente de Plataforma,* Incisos 5 y 11 de la Política Núm. ATl-011, *Mejores Prácticas de Infraestructura Tecnológica* de la Carta Circular Núm.140-16, establece que:

> *Plataforma*
>
> *La política del componente de Plataforma pretende que los dispositivos que se implementen en las agencias provean interoperabilidad y sean de uso común en la industria. Los componentes de plataforma son Servidores, Unidades de Almacenamiento y Estaciones de Trabajo (Clientes).*
>
> *Política para el Componente de Plataforma*
>
> *[…]*
>
> *(5) La planificación, diseño, adquisición e implementación de los dispositivos pertenecientes al componente de plataforma son guiados por los siguientes principios con el propósito de apoyar la estrategia de gobierno, sus metas y objetivos.*
>
> *[…]*
>
> *(11) La infraestructura de la plataforma debe ser diseñada para permitir crecimiento, flexibilidad y adaptabilidad.*

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Podría poner en riesgo los sistemas de información computadorizados y las operaciones principales del DTOP, así como la red de comunicaciones de la ACT como del propio DTOP.

2. Podría resultar en perdida de información por falla y falta de actualizaciones.

3. Carece de asistencia o piezas de reparación del fabricante ante alguna eventualidad.

Causa

Las situaciones comentadas se atribuyen a:

1. La falta de un Plan Estratégico de Tecnología por parte de la ACT y el DTOP para considerar los aspectos básicos necesarios relacionados, entre otras cosas, con los proyectos, el capital humano, la infraestructura, disposiciones legales, el plan para la renovación de los ***equipos obsoletos*** y bienes y servicios.

2. La ACT y el DTOP no realizan evaluaciones de riesgo que estén atados directamente con la planeación estratégica de la tecnología de información.

Ver recomendaciones 1 y 2

Hallazgo 2 - Falta de un Plan Estratégico de Tecnología de Información

Situación

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI[3].

Se solicitaron los planes estratégicos de tecnología de información al DTOP y la ACT. De la información suministrada por ambas entidades gubernamentales, reveló que DTOP y la ACT no cuenta con un Plan Estratégico de Tecnología de Información que este alineado con el Plan Estratégico del DTOP 2021-2024. El Plan Estratégico de DTOP 2021-2024, sometido para el año 2021 a la Oficina de Gerencia y Presupuesto no contempla estrategias o proyectos de tecnología de información.

Por otra parte, el documento titulado Plan Estratégico de Tecnología preparado el 6 de octubre de 2022, que sometió la ACT para nuestra evaluación no considera los aspectos básicos necesarios para un plan estratégico de tecnología de información, tales como: proyectos, capital humano, infraestructura, disposiciones legales, el plan para la renovación de los *equipos obsoletos* y bienes y servicios. El referido documento solo especifica la migración del *DAVID+* a los servicios en la nube de *Microsoft Azure (Cloud MS Azure)*, recomendada por la *Puerto Rico Innovation & Technology Service* (en adelante, PRITS) y presenta una propuesta emitida para la referida migración por la compañía contratada para el soporte técnico del sistema David+ Softek.

Criterio

La situación comentada es contraria al Artículo 12 *Deberes y Responsabilidades de las Agencias,* Apartado (c) de la Ley Núm. 75-2019 que establece lo siguiente:

[3] *IT Governance Institute, COBIT* ***(Control Objetives for Information and Related Technology)*****,** Descripción del Proceso, P01 Definir un Plan Estratégico de TI, Página 29.

> *Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, las agencias tendrán que cumplir con los siguientes deberes y responsabilidades:*
>
> ***(c)** Preparar y presentar a la Puerto Rico Innovation and Technology Service los planes estratégicos de las agencias y el presupuesto de éstas relativo, únicamente, a las tecnologías de información y comunicación, dentro del término establecido por la Puerto Rico Innovation and Technology Service.*

De la misma manera, el Artículo 13 *Oficial Principal de Informática de las agencias,* Apartado (a), de la mencionada ley, establece lo siguiente:

> *Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, el Oficial Principal de Informática de cada agencia, o en su defecto, el director o directores de información y tecnología de toda agencia, tendrán que cumplir con las políticas, protocolos, guías operacionales dispuestas por el PEII y los siguientes deberes y responsabilidades:*
>
> *(a) Establecer un plan estratégico y funcional para el desarrollo, la implantación y el mantenimiento del sistema de información de la agencia.*

Así mismo, el Formulario PRITS - *003 Informe Trimestral de Plan Estratégico*, establece en la Sección de Instrucciones lo siguiente:

> *Toda Agencia actualizará su informe trimestralmente luego de haber presentado ante PRITS la información desglosada en cada sección mediante informe inicial. El informe inicial deberá someterse en o antes del 30 de abril 2021.*

Efecto

La situación comentada, podría tener, entre otros los siguientes efectos:

1. El ATI de la ACT quien administra el Sistema DAVID+ del DTOP no podrá visualizar la situación actual de la entidad.
2. No crea una visión de tecnología alineada con la estrategia de la entidad.
3. No se puede identificar las oportunidades de mejora, y el rol que la tecnología debe tener en el DTOP y la ACT.
4. El DTOP y la ACT no minimizan los riesgos de una transformación tecnológica debido a la ausencia de la capacidad de cambios y los desafíos a enfrentar.
5. El DTOP y la ACT no se centran en las áreas críticas para alcanzar la misión con éxito.

6. El DTOP y la ACT no permiten identificar oportunamente estrategias para la optimización y actualización de sus equipos tecnológicos. *(***Ver Hallazgo 1***)*

Causa

La situación comentada se atribuye en gran medida, a que la secretaria del DTOP, no había requerido a la ACT la realización, para su firma, de un Plan Estratégico de Tecnología de Información, que incluye las instrucciones incluidas en el Formulario PRITS – 003, según esto se requiere en la Ley Núm. 75-2019, para la continuidad de las funciones esenciales aplicables al DTOP y a todas las dependencias adscritas, incluso la ACT.

Ver recomendaciones 1 y 2 b

Hallazgo 3 - Falta de un análisis de riesgos de los sistemas de información computadorizados y un Plan de Seguridad

Situación

El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información existentes en el DTOP, administrados por la ACT, sus vulnerabilidades y las amenazas a las que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas.

Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implementados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo y proteger dichos activos, de manera que no se afecten adversamente las operaciones del DTOP y la ACT. Mediante este proceso, se asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de ambas entidades y que respondan a las amenazas que puedan ser identificadas. Además, el análisis de riesgos debe realizarse, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

Los planes de seguridad informática son medidas que deben tomarse para proteger los recursos de la agencia y minimizar los riesgos informáticos. Pueden incluir acciones sencillas, como cambiar las contraseñas de vez en cuando, o tareas más complicadas, como hacer una copia de seguridad periódica de los recursos. El mismo deberá al menos contar con: Identificación de los activos de la organización, evaluación de riesgos y priorización de amenazas y acciones a llevar a cabo para la protección, entre otros.

El Departamento de Seguridad Nacional de Estados Unidos (*United S*tates *Department of Homeland Security*, *DHS*, por sus siglas en inglés) comenzará a hacer cumplir la ley de REAL ID (*REAL ID Act.*[4]) el 7 de mayo del 2023. El plazo anterior era el 1º de octubre del 2021, que se

[4] *The Act established minimum security standards for license issuance and production and prohibits certain federal agencies from accepting for certain purposes driver's licenses and identification cards from states not meeting the Act's minimum standards.*

consideró no viable debido a la pandemia del COVID 19 y a la desorganización que ocasionó la falta de capacidad de los estados y los territorios de emitir licencias de conducir compatibles con el *REAL ID Act*. Nuevamente, se pospuso el plazo para el 7 de mayo de 2025, esto como objetivo, dar a los estados "el tiempo necesario para garantizar que sus residentes puedan obtener una licencia Real- ID". Para los trámites, se tiene que llevar la documentación en persona a las oficinas del Departamento de Vehículos Motorizados (DMV por sus siglas en inglés), en Puerto Rico sería al Departamento de Transportación y Obras Públicas (DTOP).

El 11 de enero de 2008, el DHS emitió el *Privacy Impact Assessment for the REAL ID Final Rule,* donde establece los requisitos mínimos para aquellos estados, territorios o posesiones de los Estados Unidos de Norte América, que emitan licencias de conducir y tarjetas de identificación. Entre otros controles, la referida reglamentación requiere, entre otras cosas, que se incorporen elementos de seguridad e información en cada tarjeta, controles previos a emitir la misma, y que se establezcan controles rígidos de seguridad física en las entidades que emiten las licencias de conducir y las tarjetas de identificación.

Como parte de la evaluación de los controles internos sobre los accesos otorgados y a la seguridad DAVID+ en el requerimiento inicial se solicitó una copia del análisis de riesgos y el Plan de Seguridad del DTOP. El examen realizado reveló que DTOP:

a. No contaba con un análisis de riesgos de los sistemas de información computadorizados. En su lugar, se nos suministró el apartado II del Manual de Sistemas y Procedimientos Administrativos y Operacionales titulado Análisis de Riesgo del Área de Tecnología de Información (ATI), con una carta de aprobación del 7 de octubre de 2022, por el director ejecutivo de la ACT. En la evaluación que realizamos de dicho Análisis de Riesgo del ATI, determinamos que no se consideraban los aspectos básicos necesarios para un análisis de riesgos, tales como: la identificación de todos los activos de sistemas de información (equipos, programas y datos) existentes en el DTOP y en la ACT, con su clasificación de acuerdo con el nivel de importancia para la continuidad de las operaciones, y, en el caso de los datos, su nivel de confidencialidad; la identificación de las vulnerabilidades y amenazas, la probabilidad de ocurrencia y el impacto de cada una de estas y las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o asumir el riesgo).

b. No cuenta con un Plan de Seguridad. En respuesta a la solicitud de una copia del Plan de Seguridad, el 12 de octubre de 2022, el director del ATI nos certificó que el Departamento de Transportación y Obras Públicas (DTOP) no cuenta con un Plan de Seguridad vigente y que se está trabajando en la creación del mismo.

Criterio

La situación comentada en el **apartado a.** es contraria al *Attachment A Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the Real*

ID Act (Anexo A Mejores prácticas para la protección de información de identificación personal asociada con la Implementación estatal de la Real ID Act) incluido en la Evaluación del impacto de la privacidad para la Regla final de REAL ID del 11 de enero de 2008, establece en la sección *Information Security Best Pratices* (Mejores prácticas de seguridad de la información)*, Section (c) Elements, Subsection 1 and Subparagraphs i to ix (Apartado (c) Elementos, Inciso 1 y sus subincisos i al iv (1 al 7) y subincisos v al ix)* que establece lo siguiente:

> (c) *Elements.*
>
> *(1) In order to develop, implement, and maintain a comprehensive information security program for purposes of implementation of the REAL ID Act's regulations, each State should include in its information security program the following elements:*
>
> *i. Conduct periodic* ***assessments of risk****, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of personally identifiable information and information systems that support the operations and assets of the State DMV necessary for implementation of the REAL ID Act's regulations;*
>
> *ii. Develop and implement policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each such information system;*
>
> *iii. Develop and implement plans to provide adequate information security for facilities, networks, information systems, or groups of information systems, as appropriate.*
>
> *iv. Develop and implement an enterprise security program that addresses all of the following areas:*
>
> 1. *System access controls, which allow only authorized persons to access the personally identifiable information.*
>
> 2. *Computer and operations management, which implements practices to protect the personally identifiable information and ensures operational in*tegrity.
>
> 3. *System development and maintenance, which develops procedures for protecting information security and privacy in coding, testing, and maintaining information systems.*

4. *Physical and environmental security, which provides safeguards to protect the locations, buildings, and areas containing the technology equipment and information resources.*

5. *Compliance, which employs methods for monitoring and auditing compliance with this Rule, as well as responding to suspected instances of non-compliance.*

6. *Personnel security, which implements controls to assure that personnel are properly vetted for handling information systems.*

7. *Asset classification and control, which categorizes personally identifiable information systems as moderate or high sensitivity and implements security procedures, including data retention and destruction methods appropriate* designated classification.

Así mismo, la Sección 37.41, *Security Plan del Real ID Act* del 2005, dispone:

6 CFR2 § 37.41 - Security plan.

(a) In General. States must have a security plan that addresses the provisions in paragraph (b) of this section and must submit the security plan as part of its REAL ID certification under § 37.55.

(b) Security plan contents. At a minimum, the security plan must address –

(1) Physical security for the following:

(i) Facilities used to produce driver's licenses and identification cards.

(ii) Storage areas for card stock and other materials used in card production.

(2) Security of personally identifiable information maintained at DMV locations involved in the enrollment, issuance, manufacture and/or production of cards issued under the REAL ID Act, including, but not limited to, providing the following protections:

(i) Reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and

integrity of the personal identifiable information collected, stored, and maintained in DMV records and information systems for purposes of complying with the REAL ID Act. These safeguards must include procedures to prevent unauthorized access, use, or dissemination of applicant in formation and images of source documents retained pursuant to the Act and standards and procedures for document retention and destruction.

(ii) A privacy policy regarding the personally identifiable information collected and maintained by the DMV pursuant to the REAL ID Act.

(iii) Any release or use of personal information collected and maintained by the DMV pursuant to the REAL ID Act must comply with the requirements of the Driver's Privacy Protection Act, 18 U.S.C.2721 et seq. State plans may go beyond these minimum privacy requirements to provide greater protection, and such protections are not subject to review by DHS for purposes of determining compliance with this part.

(3) Document and physical security features for the card, consistent with the requirements of § 37.15, including a description of the State's use of biometrics, and the technical standard utilized, if any;

(4) Access control, including the following:

(i) Employee identification and credentialing, including access badges.

(ii) Employee background checks, in accordance with § 37.45 of this part.

(iii) Controlled access systems.

(5) Periodic training requirements in -

(i) Fraudulent document recognition training for all covered employees handling source documents or engaged in the issuance of driver's licenses and identification cards. The fraudulent document training

program approved by AAMVA, or other DHS approved method satisfies the requirement of this subsection.

(ii) Security awareness training, including threat identification and handling of SSI as necessary.

(6) Emergency/incident response plan;

(7) Internal audit controls;

(8) An affirmation that the State possesses both the authority and the means to produce, revise, expunge, and protect the confidentiality of REAL ID driver's licenses or identification cards issued in support of Federal, State, or local criminal justice agencies or similar programs that require special licensing or identification to safeguard persons or support their official duties. These procedures must be designed in coordination with the key requesting authorities to ensure that the procedures are effective and to prevent conflicting or inconsistent requests. In order to safeguard the identities of individuals, these procedures should not be discussed in the plan and States should make every effort to prevent disclosure to those without a need to know about either this confidential procedure or any substantive information that may compromise the confidentiality of these operations. The appropriate law enforcement official and United States Attorney should be notified of any action seeking information that could compromise Federal law enforcement interests.

(c) Handling of Security Plan. The Security Plan required by this section contains Sensitive Security Information (SSI) and must be handled and protected in accordance with 49 CFR part 1520.

Además, la Sección *Política* de la Política Núm. ATI-015, *Programa de Continuidad Gubernamental*, de la Carta Circular Núm. 140-16 establece que:

Toda agencia adscrita a la Rama Ejecutiva del Gobierno de Puerto Rico deberá seguir las siguientes políticas de continuidad establecidas. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables para cumplir la política aquí delineada.

Área de Tecnologías de información

El Área de Tecnologías de Información (ATI) de la Oficina de Gerencia y Presupuesto, establece la estructura y formatos relacionados con los informes, programas y procedimientos que forman parte del Programa de Continuidad Gubernamental:

1. *...*
2. *....*
3. *Formato para un **Análisis de Riesgos**. [Énfasis nuestro]*

Así mismo, el Apartado C *Análisis de Riesgos - Risk Analysis (RA)* de dicha política establece que:

C. Análisis de Riesgos - Risk Analysis (RA)

El Análisis de Riesgos es un informe gerencial en el cual se establece el nivel de vulnerabilidades ante la exposición de riesgos y la efectividad de los controles existentes de la agencia. También provee información crítica para la elaboración del Programa de Manejo de Emergencias. Como parte del Programa de Continuidad Gubernamental se establece que:

1. *Todas las agendas deben realizar Análisis de Riesgo dentro de un límite mínimo de tiempo de 24 meses y/o cuando se realice un cambio significativo dentro de su infraestructura operacional.*
2. *El desarrollo y análisis de los resultados del Análisis de Riesgos deberá ser certificado de acuerdo con las prácticas profesionales de continuidad establecidas para el Disaster Recovery Institute International (DRII).*

La Política para la Seguridad Cibernética aprobada el 29 de octubre de 2021, por el director ejecutivo de la *Puerto Rico Innovation Technology Service* (PRITS) establece en su Capítulo 6 Política, Apartado 6.1 Requerimientos Generales, Incisos 6.1.8, Capitulo 7 Responsabilidades, Apartado 7.2 Equipo de manejo de riesgos y seguridad cibernética Inciso 7.2.2 que:

6. Política

6.1 Requerimientos generales

Las agencias deberán:

6.1.8 Realizar evaluaciones periódicas del riesgo y la magnitud del daño que podría resultar del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la

información y los sistemas de información que respaldan las operaciones y los activos de la agencia.

7. Responsabilidades

7.2 Equipo de manejo de riesgos y seguridad cibernética

Cada jefe de la agencia debe designar a una persona o equipo que será responsable de la seguridad cibernética y el manejo de riesgos de la agencia. Las responsabilidades de este equipo incluyen, entre otras, las siguientes:

7.2.2 Evaluar el riesgo y el impacto que podría resultar del acceso no autorizado, la utilización, la divulgación, la interrupción, la modificación o la destrucción de la información o los sistemas de información.

Efectos

La ausencia de un análisis de riesgo le impide al DTOP y a la ACT lo siguiente:

1. Estimar el impacto que los elementos de riesgos que tendrían sobre los sistemas de información, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

2. Dificulta desarrollar un plan de continuidad de negocios para poder establecer aquellas medidas de control que minimicen, mitiguen o eliminen los riesgos identificados. (**Ver Hallazgo 5**).

3. Impide que se establezcan los procedimientos para restablecer las operaciones del DTOP, como las de la ACT, de surgir alguna eventualidad.

4. Se podrían detener los servicios que se le brindan al pueblo y a las partes interesadas.

La ausencia del Plan de Seguridad en el DTOP puede ocasionar, entre otras cosas, lo siguiente:

1. Se compromete la privacidad de la información personal de los individuos.

2. Aumentar la probabilidad de ocurrencia de transacciones fraudulentas.

3. Aumenta la probabilidad de ocurrencia en el uso no autorizado de las licencias de conducir y de las tarjetas de identificación que expide el DTOP.

4. Ocasiona el acceso no autorizado al Sistema DAVID+.

5. Se pone en descredito el buen nombre del DTOP ante la opinión pública.

6. La ciudadanía pierde la confianza en las instrumentalidades gubernamentales.

7. La pérdida de fondos federales.

Causa

1. La ausencia de un análisis de riesgo según indicó el director del Área de Tecnología de Información de la ACT se atribuye a la falta de recursos humanos en el área.

2. La ausencia del Plan de Seguridad se atribuye a que:

   a) El DTOP no ha iniciado ni completado la preparación de un Plan de Seguridad.

   b) El DTOP no ha observado las mejores prácticas de seguridad informática, según esto es requerido por la ley del *REAL ID ACT*.

Ver recomendaciones 1, 2c, 2d

Hallazgo 4 – Deficiencias en el Plan de Contingencias del Área de Tecnología de Información

Situación

Un Plan de Contingencia de Tecnología de Información representa una amplia gama de actividades destinadas y dirigidas a mantener y recuperar los servicios críticos después de una emergencia; éste se ajusta en un entorno mucho más amplio de preparación para emergencias que incluye la organización, la continuidad de procesos y la planificación de la recuperación. El Plan de Contingencia reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la entidad. Este Plan permite minimizar las consecuencias en caso de algún incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

1. Antes, como un plan de prevención para mitigar los incidentes.

2. Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.

3. Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

Las entidades gubernamentales, independiente de su tamaño y funciones, deben contar con un Plan de Contingencias, escrito y autorizado por el funcionario principal o el que este delegue, para restablecer sus operaciones más importantes y críticas en caso de que surja una emergencia. Dicho

Plan debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de sus sistemas de información computadorizados.

Mediante el requerimiento de información inicial (RI-001) del 21 de septiembre de 2022, solicitamos copia del Plan de Contingencia del DTOP vigente al período de examen. Como resultado de dicho requerimiento, al 7 de octubre de 2022, el ATI de la ACT contaba con un Plan de Contingencia (Plan), revisado al 18 de junio de 2009, por el director ejecutivo.

El examen realizado al Plan reveló que este no estaba actualizado y no incluía los siguientes requisitos que son necesarios para atender las situaciones de emergencia:

1. Una lista de empleados claves para reestablecer los servicios críticos y esenciales. La lista de empleados claves incluidos para el restablecimiento de los servicios incluía ochos nombre de servidores públicos de las cuales siete son exempleados.

2. No está atemperado con los servicios del **alojamiento virtual y el soporte de servicios técnicos** que fue pactado y acordado con una compañía privada para la aplicación DAVID+[5].

3. No está atemperado con los servicios de almacenamiento, acarreo y resguardo (*Data Storage Centers*) pactados y acordados con la compañía *Infokeepers of PR DBA Data Storage Centers*[6].

4. No está atemperado con los servicios para el apoyo en la administración de la base de datos Oracle, el desarrollo de aplicaciones y para el mantenimiento de la base de datos de DAVID+, que fue pactado y acordado con la compañía una *LLC*[7].

5. No está atemperado con los servicios para dar mantenimiento y soporte informático a los servidores especializados que albergan la aplicación del sistema DAVID +, sus ambientes de prueba y producción de la Directoría de Servicios al Conductor (DISCO), pactado y acordado con una compañía privada[8].

6. No está atemperado con las directrices generales emitidas por la OGP en su Política Núm. ATI-015[9] *Programa de Continuidad Gubernamental*, que permitirán a las agencias establecer un programa adecuado para garantizar la continuidad operacional de las funciones críticas que la agencia maneja, como lo es DAVID+.

[5] Contrato Núm. 2021-000143 firmado el 30 de septiembre del 2020.
[6] Contrato Núm. 2023-000013 firmado el 1 de julio de 2022.
[7] Contrato Núm. 2023-000018 firmado el 8 de julio de 2022.
[8] Contrato Núm. 2023-000036 firmado el 29 de julio de 2022.
[9] Hoy administrada por la (PRITS).

7. No identifica convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una contingencia o una emergencia. (**Ver Hallazgo 5**)

8. Las estrategias para mitigar, preparar, recuperar y responder a los riesgos incluidos en el Plan[10] no mencionan o incluyen los siguientes requerimientos que son esenciales para atender situaciones de emergencia:

    a. Una relación detallada de las configuraciones de los equipos y aplicaciones críticas, la descripción del contenido de los resguardos, ni la identificación de las librerías y archivos.

    b. Procedimientos a seguir para restaurar los resguardos.

    c. Procedimientos a seguir cuando el centro de cómputos no pueda restaurar operaciones para recibir y transmitir información.

    d. Para el período de nuestro examen, no se habían efectuado pruebas o simulacros para validar la efectividad, eficacia y mantenimiento (actualizaciones) del *Plan*.

Criterios

Las situaciones comentadas son contrarias a Sección IV *Disposiciones Generales*, Apartados A y E y a la Sección V *Alcance y Descripción del Plan de Contingencia*, Apartados C (1), D, E (1b y c), e I del Plan donde establece lo siguiente:

IV. Disposiciones Generales

A. El Director del Área de Tecnologías de información será responsable de constatar la implantación y mantenimiento de este plan.

B. ...

C. ...

D. ...

E. Será responsabilidad del Administrador del Sistema, administrar cualquier enmienda a este plan, para lo cual proveerá acceso al sistema, a la Oficina de Organización y Métodos. ...

V. Alcance y Descripción del Plan de Contingencia.

[10] Tipos de Emergencias: Huracanes, inundaciones, colapso de sistemas de energía, sismos, incendios, averías en equipo, daños causados por el hombre.

A. ...

B. ...

C. Identificación de Recursos

1. Lista de Personal Clave

D. Identificación de Equipo y Aplicaciones Criticas.

E. Asignación de Responsabilidades

Para el buen funcionamiento y efectividad de este plan es necesario que el personal clave o imprescindible para su implementación debe estar claramente designado. ...

1. Director de Área

a. ...

b. Mantenimiento del Plan

c. Establecer Centro Alterno

F. ...

G. ...

H. ...

I. Pruebas a Resguardos

Las pruebas a los resguardos constituyen un elemento esencial para comprobar que estos son confiables. Ver Tabla I y Anejo para formulario Prueba del Sistema de Resguardo.

La Política Núm. ATI-015 de la Carta Circular Núm. 140-16, dispone las guías que regirán el Programa de Continuidad Gubernamental con el objetivo de establecer con antelación la planificación y preparación necesaria, para minimizar perdidas y preservar la continuidad de todas las funciones críticas de las agencias adscritas a la Rama Ejecutiva del Gobierno de Puerto Rico ante la eventualidad de un incidente que pueda interrumpir sus operaciones y que pueda crear un estado de emergencia o desastre.

De igual manera, las situaciones comentadas no son cónsonas con las mejores prácticas en el campo de la tecnología de información que son utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados. Estas recomiendan que como parte del *Plan de Continuidad de Negocios (BCP por sus siglas en inglés)*

se deberá preparar un *Plan de Contingencias*. Como ejemplo de ello, el *Federal Information System Controls Audit Manual* (FISCAM), promulgado por el *Government Accountability Office* (GAO), establece en su Capítulo 3.5, *Contingency Planning, lo siguiente:*

> *Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.*
>
> *Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises.*

Efectos

Las situaciones comentadas propician, entre otras, lo siguiente:

1. Desorganización en caso de emergencias.
2. La improvisación por falta de guías.
3. La toma de decisiones inapropiadas.
4. Erogación innecesaria de fondos públicos.
5. Interrupciones prolongadas.
6. Ausencia de servicios al pueblo.

Causa

Las situaciones comentadas se atribuyen en gran medida a que los servidores públicos que actuaron como directores del ATI para el periodo de examen y fechas anteriores y posteriores no se aseguraron de que se incluyeran en el Plan los requisitos que son necesarios para atender las situaciones de emergencia, no lo actualizaron para atemperalos a las situaciones actuales del ATI.

Además, no requirieron que se efectuaran pruebas o simulacros al Plan para asegurarse de que este fuera uno funcional.

Ver recomendaciones 1, 2 e, f, g

Hallazgo 5- Falta de un centro alterno para la recuperación de las comunicaciones

Situación

Como parte integral del plan de continuidad de negocios (BCP, por sus siglas en inglés) de toda entidad gubernamental, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una contingencia o emergencia. En dichos convenios debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios.

Para el período examinado la ACT y el DTOP no habían formalizado un acuerdo escrito con otra entidad gubernamental para establecer en las instalaciones de ésta, un centro alterno de sistemas de información que permita restaurar las comunicaciones. En una entrevista realizada al director de la ATI de la ACT, éste les indicó a nuestros auditores que en estos momentos no contaba con un centro alterno y tampoco tenían un centro de recuperación en caso de desastres. Les indicó además que están trabajando en ello.

Criterio

La Sección V *Alcance y Descripción del Plan de Contingencia,* Apartado E (1c) del Plan de Contingencias del ATI, aprobado el 18 de junio de 2009, por el entonces director ejecutivo de la ACT, establece lo siguiente:

E. Asignación de Responsabilidades

> *Para el buen funcionamiento y efectividad de este plan es necesario que el personal clave o imprescindible para su implementación debe estar claramente designado. Así mismo, este debe tener claramente definidas sus responsabilidades para que no haya dudas o dilación en el desempeño de las mismas.*
>
> *1. Director de Área*
>
> *a. ...*
>
> *b. ...*
>
> *c. Establecer Centro Alterno*

En la Sección *Política*, apartados A, B, E y M de la Política Núm. ATI-015, se establece lo siguiente:

> *A. Desarrollo de Políticas de Continuidad*
>
> *1. Se establece que todas las agencias deben establecer políticas de continuidad conducentes a lograr el cumplimiento con ATI*[11].
>
> *2. Será responsabilidad de cada agencia de seguir y cumplir con la metodología de continuidad establecida tomando en cuenta las características propias de la agencia en base a sus operaciones y de los ambientes de tecnología existentes.*
>
> *B. Estructura de Continuidad*
>
> *1. Es requerido que cada agenda establezca una estructura organizacional de continuidad. Los directores de las agencias serán los líderes del programa de continuidad de la agencia y serán responsables de la implantación y cumplimiento del programa en la agencia. El líder de continuidad asignará un coordinador de continuidad el cual será responsable para el desarrollo de todas las actividades y ejecución del programa de continuidad de la agencia.*
>
> *E. Plan de Continuidad Gubernamental - Business Continuity Plan (BCP)*
>
> *El Plan de Continuidad Gubernamental son las tareas, actividades y procedimientos formales que ejecuta las diferentes unidades de la agenda conducentes al restablecimiento de los sistemas críticos de procesamiento ante la eventualidad de un desastre y/o contingencia. Como parte del Programa de Continuidad Gubernamental se establece que:*
>
> *1. ...*
>
> *2. El Plan de Continuidad Gubernamental deberá tener establecido las estrategias de respuesta, recuperación, reanudación y de restauración para todos los procesos críticos de las unidades de la agencia. Las estrategias de continuidad establecidas por la agenda estarán basadas en los resultados obtenidos en el informe del Análisis de lmpacto.*
>
> *3. ...*

[11] Estas funciones fueron transferidas a PRITS.

4. *El Plan de Continuidad Gubernamental deberá incluir la documentación de los procedimientos de respuesta, recuperación, reanudación y restauración de las diferentes unidades de la agencia.*

M. Personal

Cada agencia será responsable de tener el personal necesario ya sea interno o contratado para diseñar y mantener el Programa de Continuidad Gubernamental.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del **Plan de Contingencias (Ver Hallazgo 4)**, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una contingencia o 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 entidad gubernamental, podrían ser los siguientes:

a. Una entidad pública o privada de similar configuración y tamaño

b. Una compañía privada dedicada a servicios de restauración

c. Un centro alterno de la propia entidad (Oficinas Regionales)

Efectos

La situación comentada podría tener los siguientes efectos:

a. Retrasa e impide una pronta restauración de las comunicaciones.

b. Priva al DTOP y a la ACT de responder ante una contingencia dejando a los ciudadanos sin los servicios que se ofrecen.

c. Afectar las funciones del DTOP y la ACT, así como los servicios de las aplicaciones que ésta utiliza para brindar servicios.

d. No tendría disponible unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento.

e. Propicia la improvisación, y que en casos de alguna contingencia u emergencia se tomen medidas inapropiadas y fuera de orden alguno.

f. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, y de interrupciones prolongadas en los servicios provistos a los usuarios y a los clientes del DTOP y la ACT.

Causa

La situación comentada se atribuye a que la secretaria del DTOP y el director ejecutivo de la ACT no había realizado las gestiones necesarias para identificar un lugar disponible y adecuado como centro alterno, y formalizar los acuerdos necesarios para la utilización del mismo en casos de una contingencia o emergencia.

Ver recomendaciones 1, 2 h

Hallazgo 6 - Falta de un plan y de un registro para el manejo de incidentes de seguridad

Situación

Toda entidad gubernamental debe desarrollar procedimientos para identificar, informar y responder a incidentes de seguridad y el manejo de estos, incluidos aquellos que causen interrupción en la prestación de sus servicios. Estos procedimientos deben identificar el personal asignado para responder a los incidentes de seguridad e incluir el tiempo máximo y mínimo de respuesta para los incidentes y debe establecer, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

Al 7 de octubre de 2022, el director del ATI de la ACT, quien administra el Sistema DAVID+, nos certificó que DTOP no tenía un procedimiento o plan para el manejo de incidentes de seguridad relacionados con sus sistemas de información computadorizados y que se está trabajando en ello. Además, el 20 de abril de 2023, el director del ATI de la ACT, quien administra el Sistema DAVID+, nos certificó que no cuentan con un Plan de Manejo de Incidentes vigente y se está trabajando en la creación del mismo.

Así mismo, el 12 de octubre de 2022, el director del ATI de la ACT, quien administra el Sistema DAVID+, nos certificó que, en este momento, el Departamento de Transportación y Obras Públicas (DTOP) no cuenta con un Registro de Incidentes vigente y que los incidentes son documentados a través de correos electrónicos y reportes descriptivos del evento.

De igual manera, el 20 de abril de 2023, el director del ATI de la ACT, quien administra el Sistema DAVID+, nos certificó que el ATI de la ACT no cuentan con un Plan de Manejo de Incidentes vigente y se está trabajando en la creación del mismo. Nos indicó, además, que cuentan con un sistema de boletos en el cual se documentan los incidentes y la información de monitoreos a los distintos sistemas.

Criterio

La situación comentada es contraria a la sección C y E de la Política Núm. ATI-015 de la Carta Circular Núm. 140-16 que establece lo siguiente:

C. Análisis de Impactó Gubernamental - Business Impact Analysis (BIA)

El Análisis de Impacto es un informe gerencial en el cual se determina los impactos cualitativos y cuantitativos a través de una interrupción en los procesos críticos. El Análisis de Impacto permite determinar los niveles de criticidad de los procesos críticos de la agencia, los requerimientos de operación y el tiempo de recuperación operacional (Recovery Time Objective - RTO) y tiempo de resguardo requerido (Recovery Point Objective - RPO). Como parte del Programa de Continuidad Gubernamental se establece que:

1. *Todas las agencias deben realizar un Análisis de Impacto dentro de un límite mínimo de tiempo de 24 meses y/o cuando se realice un cambio significativo dentro de su infraestructura operacional.*

2. *El desarrollo y análisis de los resultados del Análisis de Impacto deberá ser certificado de acuerdo a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).*

E. Plan de Manejo de Incidentes

Un Plan de Manejo de Incidentes es una serie de actividades documentadas que serán ejecutadas por los diferentes grupos de continuidad de una agencia en respuesta a un incidente que interrumpa la prestación de sus servicios por un periodo determinado de tiempo. Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. *Desarrollar una estructura en la agencia para el Manejo de Incidentes.*

2. *Desarrollar procedimientos para detectar, reportar y responder a cualquier tipo de incidente que cause interrupción en la prestación de sus servicios.*

3. *Asegurarse que todos sus empleados, visitantes y contratistas ejecuten los procedimientos de manejo de incidentes establecidos.*

4. *La elaboración e implantación del Plan de Manejo de Incidentes deberá ser basado conforme a las prácticas*

profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

Efectos

1. La situación comentada podría provocar la duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

2. No contar con el Plan de Manejo de Incidentes no permite al DTOP y la ACT mitigar lo antes posible el impacto de incidentes sobre los usuarios y las agencias y lograr la continuidad de los servicios sin importar la severidad del incidente.

3. Limita comunicar el impacto del incidente tan pronto como se detecte, para activar la alarma y poner en práctica un plan de comunicación adecuado.

Causa

El director del ATI atribuyó la situación comentada a la falta de personal. También atribuimos esta situación a que la Oficina de Auditoría Interna de la ACT no había efectuado auditorías de los controles y la seguridad en las operaciones de los sistemas de información computadorizados, según esto nos fue certificado el 26 de septiembre de 2022, por el Auditor Interno de la ACT.

Ver recomendaciones 1, 2 i y 6

Hallazgo 7 – Incumplimiento en someter el nombramiento del Oficial Principal de Informática al PRITS

Situación

Es política pública del Gobierno de Puerto Rico que las tecnologías de información y comunicación sean administradas de forma tal, que se alcance un nivel óptimo de eficiencia, se solucione el problema de integración entre las tecnologías de información y comunicación de las agencias gubernamentales, y se facilite así el intercambio de información, se fomente la transparencia en la información y la ejecución del Gobierno, se expanda la disponibilidad y el acceso a los servicios gubernamentales, se promueva la interacción de nuestros habitantes con las tecnologías de información y comunicación, y se fomenten las iniciativas públicas y privadas que propendan a eliminar la brecha digital en nuestra sociedad.[12]

A esos efectos, las agencias gubernamentales bajo la jurisdicción de la *Puerto Rico Innovation and Technology Service (PRITS)* tenían hasta el 22 de abril de 2021, para someter una serie de documentos requeridos por la Ley Núm. 75-2019*,* según enmendada, conocida como *Ley de la*

[12] Artículo 2. — *Declaración de Política Pública* de la Ley Núm. 75-2019, según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service" (PRITS).*

Puerto Rico Innovation and Technology Service, de aquellos empleados públicos que se encuentra ocupando la plaza de OPI o ejerciendo dichas funciones.

El examen efectuado de los controles administrativos e internos relacionados con el nombramiento del Oficial Principal de Informática del DTOP y la ACT por ser ésta última la entidad que administra el Sistema David+, reveló lo siguiente:

1. El 10 de enero de 2023, nuestros auditores le solicitaron al director del Área de Tecnología de Información de la ACT y del DTOP copia del formulario PRITS-002- *Nombramiento de OPI*, mediante los requerimientos de información número 10 y 11, respectivamente.

2. El 20 de enero de 2023, el director de la Oficina de Sistemas de Información de la ACT, mediante certificación escrita les informó a nuestros auditores, entre otras cosas, que, y citamos:

> *Infiero que posteriormente, por omisión involuntaria, no se sometió el documento ni el resume que debió acompañarlo.*

3. El 23 de enero de 2023, el director de la Oficina de Sistemas de Información del DTOP, mediante correo electrónico les informó a nuestros auditores, entre otras cosas, que, y citamos:

> *El requerimiento (1) copia del formulario PRITS-002, no lo tengo disponible, en la creación e implementación de la Oficina del PRITS fueron sometidos los documentos según fueron solicitados o requeridos en ese momento por dicha oficina.*

Criterio

El Artículo 12 *Deberes y Responsabilidades de las Agencias*, en los apartados (b), (d) y (j) de la Ley Núm. 75-2019 se establece que:

> *Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, las agencias tendrán que cumplir con los siguientes deberes y responsabilidades:*
>
> *(b) Proveer y divulgar a la Puerto Rico Innovation and Technology Service, en el tiempo requerido, aquella información, datos, documentos y servicios necesarios y esenciales que les sean requeridos por la Puerto Rico Innovation and Technology Service, salvo que la divulgación requerida esté expresamente prohibida por ley o reglamento.*
>
> *(d) Cumplir con lo dispuesto en la presente Ley, las políticas de manejo de información y los estándares tecnológicos relativos a las*

tecnologías de información y comunicación que adopte y promulgue la Puerto Rico Innovation and Technology Service.

(j) Notificar todo nombramiento de Principales Oficiales de Informática al PEII para su evaluación y recomendación final.

La Sección 4ta del Boletín Administrativo Núm. OE-2021-007, *Orden Ejecutiva del gobernador de Puerto Rico, Hon. Pedro R. Pierluisi, para decretar como política pública la aceleración del gobierno digital, el desarrollo de la intercomunicación e interoperabilidad de los sistemas de tecnología del gobierno*, emitido el 4 de enero de 2021, establece, entre otras cosas, lo siguiente:

[….]

Por su parte, se apercibe a los jefes de agencia que además de lo dispuesto en esta Orden Ejecutiva, deberán cumplir con todos los deberes que les impone la Ley Núm. 75-2019.

Asimismo, el mencionado Boletín Administrativo Núm. OE-2021-007, establece en su Sección 5ta *Nombramientos de los principales oficiales de informática*, lo siguiente:

En aras de lograr la mejor coordinación de planificación e implementación de estrategias y planes tecnológicos y de innovación, y en cumplimiento con las disposiciones de la Ley Núm. 75-2019, todo nombramiento de algún Principal Oficial de Informática en una agencia, corporación pública y/o instrumentalidad del Gobierno de Puerto Rico, deberá ser notificado al PEII para su evaluación y recomendación final.

Por otra parte, la Orden Administrativa Núm. PRITS 2021-003, emitida el 12 de abril de 2021, por la PRITS, sobre *Establecer las directrices sobre nombramiento(s) de oficial(es) principal(es) de informática (OPI) de las agencias bajo la jurisdicción de Puerto Rico Innovation & Technology Service en cumplimiento con la Ley 75-2019*, establece en su Tercer Por Cuanto, Apartado 5 que:

La Ley-75 crea una serie de funciones, facultades y deberes tanto de PRITS, el PEII, el Principal Oficial de Informática del Gobierno, y cada Oficial Principal de Informática ("OPI") de las Agencias bajo jurisdicción de PRITS. En particular el Articulo 6 de la Ley-75, autoriza a PRITS, entre otras las siguientes actuaciones:

[…]

5. Evaluar y emitir recomendación final en los nombramientos de los Principales Oficiales de Informática de las Agencias. Véase, Art. 6(ee) de la Ley-75.

De igual forma, la mencionada Orden Administrativa Núm. PRITS 2021-003, establece primero lo siguiente:

Con el propósito de apoyar a las Agencias en dar fiel cumplimiento a las disposiciones de la Ley-Núm.75 y para que PRITS pueda encaminar una integración adecuada de las TIC[13], así como maximizar los recursos tecnológicos y capital humano del Gobierno toda Agencia presentará lo siguiente mediante la utilización del Formulario ***PRITS-002 - NOMBRAMIENTOS DE OPI:***

> ***NOMBRAMIENTOS OFICIAL(ES) PRINCIPAL(ES) DE INFÓRMÁTICA (OPI):*** *Dentro de un término no mayor a* ***10*** *días de entrar en vigor esta Orden Administrativa, se habrán de someter, los siguientes documentos de la persona que se encuentra ocupando la plaza de OPI o ejerciendo dichas funciones:*
>
> *a. Resume o currículum.*
>
> *b. Indicar si el OPI es empleado de carrera en dicha plaza o si es objeto de algún destaque, licencia, etc.*
>
> c. *Cualquier otro documento que la autoridad nominadora de la agencia estime necesario.*
>
> *No podrá hacerse nombramiento, transferencia, destaque de ninguna persona como OPI sin la previa autorización de PRITS. De lo contrario, estos podrán declararse nulos.*

Efecto

La situación comentada podría tener, entre otros, los siguientes efectos:

1. Incumplimiento con la *Ley de la Puerto Rico Innovation and Technology Service.*
2. Podrían existir limitaciones en el cumplir con las políticas, protocolos, guías operacionales dispuestas por el PEII y los deberes y responsabilidad es establecidos por la PRITS hacia los OPI.

Causa

1. En relación con la ACT el director del Área de Tecnología de Información atribuyó la situación a la omisión involuntaria.
2. En relación con el DTOP el director de la Oficina de Sistemas de Información atribuyó la situación a la localización de los documentos.

[13] TIC. — Significa las tecnologías de información y comunicación.

Ver recomendaciones 1 y 3

Hallazgo 8 - Falta de organización de los cables que se conectaban a los equipos de comunicación

Situación

a. La red de comunicaciones del DTOP y la ACT contaba con un cuarto de comunicaciones (*Minillas Data Center*) en el segundo piso y 18 cuartos de distribución de cableado, entre los 18 pisos de la Torre Sur del Centro Minillas. En estas áreas se habían instalado estantes para organizar y proteger los equipos de comunicación que mantenían las conexiones necesarias para interconectar las computadoras que recibían servicio de la red.

   El examen efectuado al 21 de noviembre de 2022 y el 7 de diciembre de 2022, sobre los controles físicos y ambientales existentes en dichas áreas reveló lo siguiente:

   1) En los 18 cuartos de cableado o el 100% no se mantenían organizados, ni identificados, ni amarrados los cables que se conectaban a los equipos de comunicación mantenidos en el *Minillas Data Center* y en los cuartos de distribución de cableado ubicado en los 18 pisos del edificio. Esto es necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones. **(Ver Anejo 1)**

   2) En los 18 cuartos de distribución o el 100% no había un diagrama esquemático ni un diagrama de los *drops*[14] que ilustrara las conexiones establecidas con los equipos.

   3) En los 18 cuartos de cableado o el 100%, del equipo de comunicación, se mantenía el panel de los cables del servicio telefónico que estaba fuera de funcionamiento. Esto dificulta mantener un control de acceso adecuado a dichos cuartos.

   4) En dos cuartos de cableados o el 11% no están en un lugar independiente permitiendo el acceso directo a cualquier persona. (**Ver Anejo 2**).

   5) Con relación a los controles ambientales examinados en 18 cuartos de distribución de cableado se determinó lo siguiente:

      a. En equipos de telecomunicaciones instalado en 9 o el 50% de los cuartos de distribución de cableado presentaban particulado de polvo acumulado, lo que denota la falta de mantenimiento.

      b. En 18 cuartos de distribución de cableado o el 100% no había acondicionadores de aire, por lo que la temperatura existente en los mismos no era adecuada.

[14] Conector de pared para las instalaciones de redes.

c. En los 18 o el 100% de los cuartos de cableados no existen controles para asegurar la existencia de niveles adecuados de temperatura y humedad.

d. En 13 de los cuartos de cableado o el 72%, los cuartos de distribución de cableado eran utilizados para almacenar materiales y otros equipos, tales como: cajas de cartón, documentos, equipos de computadoras y una escalera de aluminio.

e. En los 18 cuartos de cableado o el 100% no cuentan con extintores de incendios.

Criterio

La situación comentada es contraria a lo establecido en la Política Núm. ATI-011*, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y uso de la Tecnológica de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016, por el director de la Oficina de Gerencia y Presupuesto (OGP); En esta se establece que las entidades gubernamentales tienen la responsabilidad de adquirir e implementar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientes. Además, se establece que las redes en las entidades deben proveer la infraestructura necesaria para implementar y mantener los procesos de negocio de la entidad gubernamental, y ser operacionales y confiables.

Asimismo, la situación presentada es contraria a las mejores prácticas y estándares de la industria donde se requiere que la gerencia 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 parte de una 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 organizados los cables que conectan los equipos de comunicación. Esto permite atender y corregir a tiempo los problemas de comunicación, y detectar cualquier conexión no autorizada. Un sistema de cable bien organizado ofrece una gran cantidad de beneficios, siendo la seguridad el más importante.

Efecto

La situación comentada puede causar, entre otros, los siguientes efectos:

1. Dificulta los trabajos realizados por el personal del ATI de la ACT para atender los problemas de conexión en un tiempo razonable.

2. No hay acceso fácil a los cables.

3. Las reparaciones y actualizaciones se hacen menos sencillas.

4. Solución de problemas menos rápida (los errores humanos son una de las principales razones del tiempo de inactividad).

5. Mayor las posibilidades de desconectar el cable equivocado.

6. Aumenta el tiempo de inactividad de la red y el daño del cable.

7. Disminuye el flujo de aire y la refrigeración, lo que puede acortar la vida útil de los cables.

8. Disminuye el rendimiento de la red con menor velocidad, eficiencia y ancho de banda.

9. Impide a la ATI 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.

10. Dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Causa

La situación comentada se debió a que el director del ATI de la ACT no había impartido instrucciones para que se organizaran los cables conectados a los equipos de comunicación y a la falta de personal que impera en la ACT y el DTOP.

Ver recomendaciones 1,2 j, 2 k 1),

Hallazgo 9 - Deficiencias relacionadas con la administración de las cuentas de acceso activas a exempleados en el Sistema DAVID+

Situación

Mantener a exempleados con cuentas activas en los sistemas de información quebranta el principio de la seguridad en los sistemas de información. Toda entidad gubernamental, independientemente de su tamaño, deben implementar controles de acceso rígidos para la utilización de la información y los programas de aplicación, de forma que estos sean accedidos solo por el personal autorizado. Las cuentas de acceso a los sistemas de información deben administrarse para controlarlas eficazmente e identificar y autenticar a los usuarios. Las agencias tienen y deben revisar periódicamente las listas de autorizaciones de las cuentas de accesos a los sistemas de información para determinar si son apropiadas. Además, las entidades deben asegurarse de que los administradores de las cuentas reciban una notificación cuando los usuarios de los sistemas de información cesan funciones o se transfieren para que se eliminen, inactiven o aseguren las cuentas de acceso asignadas.

Para garantizar la seguridad de la información almacenada en el Sistema David+ y limitar el acceso a información privilegiada y protegida, el DTOP y la ACT deben eliminar los accesos al sistema

computadorizado, de los empleados y contratistas que ya no trabajan o no tengan relación contractual con estos. La seguridad de datos, también conocida como seguridad de la información, seguridad informática o ciberseguridad es un aspecto esencial de la tecnología de información en entidades de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de unos posibles actos de corrupción o irregularidades durante todo su ciclo de vida**.**

El examen realizado con 214 empleados que cesaron funciones durante el 1 de julio de 2021 al 31 de agosto de 2022, según la información sometida por la Oficina de Recursos Humanos del DTOP, reveló que 2 cuentas, pertenecientes a 2 exempleados, permanecían activas. Uno de estos renunció al 30 de junio de 2022 y a la fecha de nuestra visita el 9 de febrero de 2023, permanecía activo con acceso a los sistemas, el otro empleado con fecha de finalización al 24 de enero de 2022, su acceso a los sistemas fue eliminado al 13 de octubre de 2022. Esto de acuerdo con una verificación ocular realizada por nuestros auditores al sistema David+ el 9 de febrero de 2023, en el DISCO de Carolina y mediante el Informe de Usuarios de empleados que se desvincularon del servicio para el período de examen.

Criterio

La Sección 6 *Política*, Apartado 6.2 *Concienciación sobre la política, comunicación y capacitación*, Inciso 6.2.3 *Salidas o cambios en la situación laboral* de la Política para la Seguridad Cibernética, aprobada el 29 de octubre de 2021 por PRITS establece que:

> 6.2. *Las agencias serán responsables de la promoción continua y concienciación sobre la seguridad cibernética a través de capacitaciones, talleres u orientaciones periódicas. Para mitigar el riesgo de eventos de ciberseguridad y la divulgación involuntaria de información confidencial por parte de los empleados y proveedores de servicios externos, se tomarán las siguientes medidas.*
>
> *6.2.3 Salidas o cambios en la situación laboral*
>
> *Tras un cambio en la situación laboral (por ejemplo, promoción, transferencia o despido), el personal de Recursos Humanos se asegurará de que se informe al Oficial Principal de Informática o al personal designado por éste para que la cuenta del empleado y los privilegios de acceso físico se restrinjan de manera oportuna, según corresponda para garantizar el acceso con privilegios mínimos.*

Como norma de control interno 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 la notificación inmediata al encargado de la seguridad del Sistema DAVID+ del cese de

un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente. Para esto, deberán establecerse procedimientos escritos y aprobados que incluyan, entre otras cosas, una comunicación efectiva entre el área de Recursos Humanos, el área en que labora el empleado y el ATI.

Efecto

La situación comentada propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta, la comisión de irregularidades (delitos) y la alteración, por error o deliberadamente, de los datos contenidos en el Sistema David+. Esto, sin que puedan ser detectados para fijar responsabilidades.

Causa

La situación comentada se atribuye a que la directora del DISCO y el personal del Área de Tecnología de Información de la ACT y la Oficina de Sistemas de Información del DTOP no se aseguraron de cancelar las cuentas de acceso al personal que cesó funciones.

Ver recomendaciones 4

Hallazgo 10 - Falta de controles físicos en el área del servidor donde reside el Sistema DAVID+

Situación

El 30 de septiembre de 2020, el DTOP formalizó el Contrato Núm. 2021-000143 con una compañía privada, con vigencia del 30 de septiembre de 2020, hasta el 30 de junio de 2025. Esto, para el arrendamiento especializado de un centro de datos para albergar los servidores, entre otros, donde reside el sistema David+, por una cuantía máxima de tres millones ciento sesenta y nueve mil doscientos dólares ($3,169,200.00).

El examen efectuado sobre los controles físicos[15] existentes en el *Datacenter Collocation* donde se mantiene el servidor que reside el Sistema DAVID+, reveló que el equipo de control de acceso físico estaba fuera de uso, según esto, fue certificado por el Gerente General de la compañía privada el 28 de agosto de 2022.

Criterio

En la propuesta *Information Technology DTOP, Datacenter Collocation and Virtual Hosting Replication Services, Technical Support Services and Network Monitoring* del 12 de febrero de 2020, la cual forma parte del referido Contrato entre la compañía privada, y el DTOP, establece

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

en la Sección del *DTOP Data Center Collocation Services, Building Infrastructure,* Apartado (9) y en *Data Center Security* lo siguiente:

- *Building infrastructure: The CBRC is in the 2,500 square foot facility in San Juan, Puerto Rico. Built to the exacting standards of the technology industry, its building infrastructure features:*

  [….]

  9) Controlled Access

- *Data center Security: Physical security is an important aspect of the (compañia privada). The CBRC is a physically secure structure with all the appropriate security features. All access is restricted.* ***Access is possible through the use of access controls cards that are provided by management.***

En la Sección 3.5 *Controles Adicionales de TI*, Apartados 3.5.3 y 3.5.16 de los *Estándares para la Seguridad Cibernética* aprobados el 29 de octubre de 2021, por el PRITS en virtud de la Ley 75-2019, se establece lo siguiente:

> *3.5.3* Las *instalaciones y activos de procesamiento de información (por ejemplo, servidores, armarios de cableado para redes, conexiones telefónicas, áreas de impresión para datos sensitivos o confidenciales) deberán estar alojados en áreas seguras, protegidas con un perímetro de seguridad apropiado y controles para evitar el acceso no autorizado y daños.*
>
> *3.5.16 El acceso a las instalaciones de los sistemas de información (por ejemplo, servidores, áreas de almacenaje de equipo) estará controlado de manera que solo el personal autorizado pueda accederlos.*

Como norma general y de control interno, toda agencia gubernamental debe mantener el acceso a las instalaciones de sistemas de información controlado para que solamente el personal autorizado pueda utilizarlas. Además, toda agencia será responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de su ambiente de tecnología, particularmente sus sistemas críticos. Esto implica que, como sana administración, las agencias deberán tomar los cuidados necesarios para proteger y mantener funcionando en óptimas condiciones los equipos electrónicos para evitar daños y averías. El propósito es asegurar la integridad, la exactitud y la disponibilidad de la información y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y sistemas computadorizados, es necesario que se controle adecuadamente el acceso de personas al área del o los servidores principales.

De igual manera, el DTOP y la ACT son responsables de desarrollar procedimientos para, entre otras cosas, detectar, informar y responder a incidentes de seguridad y deben ser implementados,

en parte, mediante la activación de todas las opciones para registrar los eventos de seguridad, y mediante la revisión continua, por el personal técnico especializado, de los registros computadorizados producidos por el equipo de control de acceso físico.

Efecto

La situación comentada puede tener como efecto lo siguiente:

1. No pudimos verificar que personas tuvieron acceso a los servidores principales del DTOP, donde reside el Sistema DAVID+.

2. Que personas no autorizadas o ajenas al ATI de la ACT y la Oficina de Sistemas de Información de DTOP, causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información.

3. Disminuye la confiabilidad de la información computadorizada.

4. Aumenta el riesgo de destrucción y divulgación indebida de la información computadorizada.

5. Dificulta la adjudicación de responsabilidades a las personas que cometan actos indebidos o accesos no autorizados.

6. Puede afectar adversamente el funcionamiento de la red y la continuidad de las operaciones.

Causa

La situación comentada se debía, en parte, a que el director del Área de Sistemas de Información de la ACT no había tomado las medidas de control necesarias para supervisar a la compañía privada, en cuanto a su cumplimiento con la protección física del *Datacenter Collocation* donde se mantiene el servidor que reside el Sistema DAVID+.

Ver recomendaciones 1 y 2 l

Hallazgo 11 - Fallas relacionadas con el diagrama esquemático de la red de comunicaciones

Situación

Las entidades gubernamentales, independientemente de su tamaño y los servicios que ofrecen a la ciudadanía, deben adquirir e implementar una infraestructura de tecnología de información segura, basada en los estándares de dominio en la industria[16], y las normas y requerimientos establecidos

[16] Los estándares de la industria asociados al dominio de Sistemas de Información definen reglas o características que facilitan el manejo de temas específicos de este dominio, entre ellos se destacan los siguientes: arquitecturas de software, encripción de datos, especificación de requerimientos,

por la *Puerto Rico Innovation and Technology Service* (PRITS), la cual proporcione la intercomunicación necesaria para la distribución eficaz de los servicios. El diseño de la red de intercomunicaciones (*Network Topology Diagram)* debe estar documentada con los diagramas esquemáticos que permitan identificar y documentar todos los dispositivos utilizados para acceder a la misma, las vías de telecomunicaciones y los usuarios de esta, entre otros. Esto, con la intención de identificar los puntos de acceso a los recursos de la red, para ser controlados. Además, el diagrama esquemático de la red de intercomunicaciones debe mantenerse actualizado.

Las operaciones del DTOP se realizan desde el edificio Sur del Centro de Gobierno Millas y está compuesto por las secretarías auxiliares de Administración y Recursos Humanos, y de Planificación, Programación y Control, y por las directorías de Servicios al Conductor, Desarrollo Comunitario, Obras Públicas, y Urbanismo. La Directoría de Obras Públicas cuenta con 7 oficinas regionales localizadas en Aguadilla, Arecibo, Guayama, Humacao, Mayagüez, Ponce y San Juan. La Directoría de Servicios al Conductor (DISCO) cuenta con 15 centros de servicios al conductor (CESCO) localizados en Aguadilla, Arecibo, Barranquitas, Bayamón, Caguas, Carolina (Metropolitano), Fajardo, Guayama, Humacao, Manatí, Mayagüez, Ponce, Río Piedras, Utuado y Vieques.

Al 3 de noviembre de 2022, a solicitud de nuestros auditores, la ACT nos sometió dos diagramas, uno como *DTOP/ACT Logical Network Diagram* revisado al 20 de abril de 2020, por un ingeniero y otro como Diagrama de Red – Servicios de Colocación**,** revisado el 12 de marzo de 2022**,** por un ingeniero. Nuestro examen sobre estos diagramas esquemático reveló lo siguiente:

1. El DTOP/*ACT Logical Network Diagram* tenía dos años de su última revisión, por lo que no estaba actualizado con los cambios en la infraestructura que se habían realizado en la ACT y el DTOP.

2. El Diagrama de Red – Servicios de Colocación**,** revisado el 12 de marzo de 2022, no incluía el detalle de las conexiones por puerto de cada ***switch***[17] de los equipos de comunicación de la ACT y el DTOP, donde presentara el rango de las conexiones activas para identificar los puntos de acceso a los recursos de la red. (**Ver Hallazgo 8**)

Es fundamental que las rutas de acceso se identifiquen y queden documentadas en un diagrama de ruta de acceso o un diagrama de red similar esquemático. Tal diagrama o esquema identifica a los usuarios del sistema, y el tipo de dispositivo desde el que pueden acceder al sistema.

planes de configuración de software, controles de seguridad de la información, ciclo de vida de los sistemas de información, calidad de software y patrones de arquitectura.

[17] Un ***switch*** o **conmutador** es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

Criterio

La situación comentada es contraria a lo indicado en la Sección de RED, Política para el Componente de Red de la *Política Núm. ATI-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular Núm. 140-16* donde se estable lo siguiente:

> *Al establecer una política del componente de Red se pretende que las agencias[18] adquieran e implementen una infraestructura de red segura, escalable, basada en estándares de dominio en la industria, la cual provee la comunicación necesaria para la distribución de servicios eficientemente.*
>
> *Política para el Componente de Red*
>
> *[…]*
>
> *4. El diseño de la red debe estar documentado.*

Efectos

La situación comentada impide a la ACT y al DTOP de lo siguiente:

1. 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.

2. Dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Causa

El director del ATI de la ACT atribuyó la situación a la falta de personal.

Ver recomendaciones 1,2k2), 2m

Hallazgo 12 - Fallas relacionadas con los controles ambientales en el *Minillas Data Center*

Situación

a. Las entidades deben establecer controles ambientales para prevenir o mitigar los daños potenciales a las instalaciones y las interrupciones en los servicios. Estos controles incluyen detectores de humo, alarmas de fuego y luces de emergencia, extintores de incendio, entre

[18] Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley Núm. 151-2004.

otros. Además, los recursos que apoyan las operaciones críticas y funciones de una entidad, incluidos los componentes de la red, deben identificarse y documentarse.

La ATI de la ACT cuenta con centro de datos (*Minillas Data Center*) donde se opera una red de comunicación que administra dos Chasis de Conmutación Hp 7506 *(HPE 7506 Switch Chassis*) la cual se conectan con dos Controladores de Acceso (*HP MSM760 Access Controller*) que permite la interconexión inalámbrica de dispositivos electrónicos (*WIFI*) y a su vez, se conectan con un enrutador (*Router*) Cisco 7606[19] utilizado para la conexión con la red de la compañía de data, la *Puerto Rico Electric Power Authority* (PREPA) Net de la OGP[20] y la retrasmisión con el sitio de la réplica (*Prime Venture Data Center*). Al mismo tiempo, los chasis de conmutación se conectan con un enrutador Cisco 2921 utilizado para manejar el Multiprotocolo de Conmutación de Etiquetas (MPLS o *Multiprotocol Label Switching)* de la compañía Claro para manejar la red de área amplia (WAN) de la ACT. Además, ambos chasis de conmutación controlan 36 conmutadores (switches HP5130 - 48G) distribuidos en los 18 pisos de la Torre Minillas Sur y esta red de comunicaciones está segmentada en 7 redes de área local virtuales **(**VLAN o Virtual LAN) protegidas por dos cortafuegos (F*irewall Fortigate500), u*n administrador de registros con visibilidad de toda la superficie de ataques (*Forti analyzer 400e*) con un punto de acceso para acceder a las redes Wi-Fi de una forma segura y centralizada *(Forti AP*).

Las inspecciones efectuadas el 9 y 21de noviembre de 2022, de los controles existentes en el *Minilla Data Center* y en las áreas dónde se mantenían los conmutadores (*switches*) revelaron lo siguiente:

1. Relacionado con los controles ambientales en el *Minilla Data Center*:

    a) No se mantiene un registro de visitantes.

    b) No existen sensores para detectar la presencia de agua.

    c) Las luces de emergencia estaban fuera de servicio según notificado por el director del ATI.

2. El cableado que 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. (**Ver Hallazgo 8 y Anejo 1**)

3. El área carecía de techos acústicos, lo que ocasiona la acumulación excesiva de polvo en los equipos.

[19] Los enrutadores de la serie Cisco 7600 se han retirado y ya no son compatibles. Fecha de fin de venta: 2016-07-24. Fecha de finalización del soporte técnico: 2021-07-31.

[20] PREPA Networks es una subsidiaria de la Autoridad de Energía Eléctrica de Puerto Rico y utiliza gran parte de su infraestructura de distribución de energía para esparcir su tecnología de fibra óptica.

Criterio

Las situaciones comentadas se apartan de lo establecido en el Capítulo 3 *Evaluating and Testing General Controls* Sección 3.5 *Contingency Planning,* Apartado *CP-2.2. Adequate environmental controls have been implemented* del FISCAM, donde establece lo siguiente:

> *Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include:*
>
> - *fire extinguishers and fire-suppression systems.*
> - *fire alarms.*
> - *smoke detectors.*
> - *water detectors.*
> - *emergency lighting;*
> - *redundancy in air cooling systems.*
> - *backup power supplies.*
> - *existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities.*
> - *processing facilities built with fire-resistant materials and designed to reduce the spread of fire; and*
> - *policies prohibiting eating, drinking, and smoking within computer facilities.*
>
> *Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages.*

Efectos

Las situaciones comentadas pueden causar lo siguiente:

1. Pueden ocasionar daños y deterioros prematuros en los equipos de la red y las computadoras, lo que podría impedir que se obtenga el rendimiento máximo en términos de los servicios que estos ofrecen.

2. El contar con equipo que se han retirado y no tienen soporte técnico **(Ver Hallazgo 1**) es probable que implique el asumir riesgos en materia de seguridad, crear interrupciones en los servicios con altos costos para DTOP, vulnerabilidad en el sistema que permiten con más facilidad los ataques cibernéticos y quebranta la seguridad en las comunicaciones.

Causa

El director de la ATI atribuyó las situaciones comentadas a que no contaba con el personal necesario.

Ver recomendaciones 1, 2 n

Hallazgo 13 - Deficiencias relacionadas con el informe de inventario de la OSI del DTOP y del ATI de la ACT y de los programas instalados en las computadoras

Situación

Los sistemas de información de las entidades gubernamentales, independientemente de su tamaño, incluidos los programas, las aplicaciones y todos los archivos electrónicos, deben constar en el inventario de las respectivas agencias y solo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente y constatarse en un documento oficial.

a. Para el período de 1 de julio de 2021 al 31 de agosto de 2022, el director de la ACT le proveyó a los auditores el inventario físico de los equipos y las configuraciones de estos ubicados en el *Datacenter Collocation* donde se mantiene el servidor donde reside el Sistema DAVID+. Pero, la ACT, para el referido período, no contaban con lo siguiente:

    1. Un inventario de los equipos computadorizados que incluyera, entre otras cosas, la descripción, el número de propiedad, la fecha de adquisición, el precio unitario y la localización.

    2. No contaban con un registro de los programas adquiridos e instalados en las computadoras que incluyera, entre otras cosas, el número de la licencia del programa, el costo de los programas instalados, el nombre del proveedor, el nombre del usuario, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado la descripción de la computadora donde están instalados los mismos y el total de licencias adquiridas.

b. El 14 de febrero de 2023, el director de la OSI del DTOP sometió un inventario de activos fijos tomado al 13 de febrero de 2023, de la propia OSI y no así de todo el DTOP. Además, no sometió el registro de los programas adquiridos e instalados en las computadoras que incluyera, entre otras cosas, el número de la licencia del programa, el costo de los programas instalados, el nombre del proveedor, el nombre del usuario, el dueño de la

licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado la descripción de la computadora donde están instalados los mismos y el total de licencias adquiridas.

Criterio

Las situaciones comentadas en los **apartados a. 1. y b.** son contrarias a lo establecido en el Artículo 10 *Custodia, control y contabilidad de propiedad pública*, Apartado (a) de la Ley Núm. 230 del 23 de julio de 1974, según enmendada, *Ley de Contabilidad del Gobierno de Puerto Rico*, que establece lo siguiente:

> *(a) La custodia, cuidado y control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia, Cuerpo Legislativo o entidad corporativa o su representante autorizado.*

Así mismo, las situaciones comentadas son contraria al Artículo XIV Inventario Físico, Apartados A y D del Reglamento 11 *Normas Básicas para el Control y Contabilidad de los Activos Fijos*, aprobado el 29 de diciembre de 2005, por el Secretario de Hacienda, donde establece lo siguiente:

> *A. Los registros internos de las dependencias de inventario tienen que estar respaldados por los inventarios físicos.*
>
> *...*
>
> *D. Las agencias prepararán el inventario de forma mecanizada utilizando el Modelo SC 795, Inventario Físico de Activo Fijo.*

Las situaciones comentadas en los **apartados a. 2. y b.** es contraria a lo establecido en la Sección de *Normas Generales Aplicables al Uso de los Sistemas de Información*, Apartado 2, Política Núm. ATI-008, *Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la Carta Circular Núm. 140-16 que dispone lo siguiente:

Normas generales aplicables al uso de los sistemas de información:

> *2. Los sistemas de información de las entidades gubernamentales, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y solo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente constatándolo en documento oficial.*

La Orden Administrativa PRITS-2021-002, emitida el 12 de abril de 2021, por el Principal Ejecutivo de Innovación e Información del Gobierno y Director Ejecutivo – PRITS, establece en

su POR TANTO PRIMERO, Artículo I Plan Estratégico, Apartado 3 Informe de Infraestructura lo siguiente:

> *Mediante la utilización de la **SECCIÓN C** del Formulario **PRITS-003 PLAN ESTRATÉGICO** se habrá proveer la siguiente información:*
>
> *a. **Desglose de los equipos***

Efectos

Las situaciones comentadas en el **apartado a.** le impiden a la ACT mantener un control efectivo sobre el equipo y la propiedad bajo su custodia. Además, propician el ambiente para el uso indebido o la desaparición de la misma, y otras situaciones adversas, sin que se puedan detectar a tiempo para fijar responsabilidades.

Las situaciones comentadas en los **apartados a. (2) y b.** impiden ejercer un control eficaz de los programas y de las licencias correspondientes. Además, pueden propiciar la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para el DTOP y la ACT.

Además, ambas situaciones dificultan y limitan nuestra gestión fiscalizadora.

Causa

Las situaciones comentadas se atribuyen a que los directores de la ATI y la OSI de la ACT y el DTOP, respectivamente, no velaron que el personal encargado de la propiedad cumpliera con su responsabilidad de mantener un inventario de la propiedad del propio DTOP y la ACT. Asimismo, los directores mencionados no habían tomado las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en las computadoras de ambas entidades gubernamentales.

Ver recomendaciones 1, 2, o, p

Hallazgo 14- Falta de adiestramientos continuos a los usuarios sobre el uso de los sistemas de información y las políticas de seguridad y otras deficiencias en la implantación de éstas

Situación

El 9 de diciembre de 2022, se cumplimentaron a 16 usuarios activos de los sistemas de información del DISCO y del CESCO de Carolina un Cuestionario[21] sobre la satisfacción de los usuarios. La

[21] En dicho Cuestionario se solicita información, entre otras cosas, de los adiestramientos tomados sobre los sistemas de información, de seguridad de la aplicación DAVID+, de las políticas de seguridad y contraseñas el uso y manejo de la internet y de la generación de reportes.

información obtenida mediante los cuestionarios y las visitas realizadas por los auditores reveló lo siguiente:

A los usuarios no se les habían ofrecido adiestramientos u orientaciones en cuanto al uso de los sistemas de información y las normas de seguridad, según se detalla a continuación:

a. Once de los usuarios (69% por ciento) no habían recibido adiestramientos en cuanto al uso de los sistemas de información.

b. Catorce de los usuarios (88% por ciento) no habían recibido adiestramiento u orientación en cuanto a las normas de seguridad establecidas en el DTOP y la ACT.

c. Quince de los usuarios (94% por ciento) no habían recibido adiestramientos sobre la preparación de los respaldos de información.

d. Trece de los usuarios (81% por ciento) no habían recibido adiestramientos sobre el uso del correo electrónico.

e. Once de los usuarios (69% por ciento) no habían recibido adiestramientos sobre el cambio de contraseña.

f. Catorce de los usuarios (88% por ciento) no habían recibido adiestramientos sobre el uso de Internet.

g. Diez siséis de los usuarios (100% por ciento) no habían recibido adiestramientos sobre los derechos de autor o piratería.

h. Diez de los usuarios (63% por ciento) desconocían las políticas de contraseñas establecidas. Ocho de estos usuarios mencionaron que al momento que el sistema solicitaba el cambio de contraseña utilizaban la misma del cambio anterior.

i. Once de los usuarios (69% por ciento) no tenían en su área de trabajo el Reglamento relacionado con la seguridad en los sistemas de información, ni el correo electrónico mediante el cual se le envió copia del mismo.

j. Dos de los usuarios (13% por ciento) no han completado algún formulario referente a los accesos y privilegios otorgados a los sistemas de seguridad.

k. Quince de los usuarios (94% por ciento) no requieren de la aprobación o autorización de un supervisor para cancelar, eliminar o modificar alguna transacción, ya que el acceso otorgado al sistema permite que lo realicen sin necesidad de alguna aprobación.

Criterio

La Ley Núm. 8-2017, según enmendada, conocida como *Ley para la Administración y Transformación de los Recursos Humanos en el Gobierno de Puerto Rico*, establece en su Sección 6.5. — *Disposiciones sobre Adiestramiento* que:

> *El adiestramiento constituye parte esencial del principio de mérito. Es indispensable atemperar la política pública en materia de adiestramientos a las realidades de la Administración Pública del Siglo XXI.*

La Carta Circular Núm. 2021-007, sobre el *Establecimiento de la política para la seguridad cibernética*, emitida el 6 de diciembre de 2021, por la *Puerto Rico Innovation Technology Service* (PRITS) establece en su ***Propósito y Determinación*, Apartado 5 que:**

> *La Política para la Seguridad Cibernética tiene como objetivo:*
>
> *1. ...*
>
> *2. ...*
>
> *3. ...*
>
> *4. ...*
>
> *5. Proporcionar orientación a empleados nuevos y existentes, personal temporero, contratistas, socios y terceros sobre la importancia de sus funciones y responsabilidades relacionadas con la seguridad cibernética y la protección de los activos de información del gobierno.*

La Política para la Seguridad Cibernética aprobada el 29 de octubre de 2021, por el director ejecutivo de la PRITS establece en su Capítulo 6 Política, Apartado 6.2 Concienciación sobre la política, comunicación y capacitación, Incisos 6.2.1 Empleados nuevos y 6.2.2 Empleados existentes, Capitulo 7 Responsabilidades, Apartado 7.4 *Puerto Rico Innovation and Technology Service* (PRITS), Inciso 7.4.1.17 que:

> 6. *Política*
>
> *6.2 Concienciación sobre la política, comunicación y capacitación*
>
> *Las agencias serán responsables de la promoción continua y concienciación sobre la seguridad cibernética a través de capacitaciones, talleres u orientaciones periódicas. Para mitigar el riesgo de eventos de ciberseguridad y la divulgación involuntaria de información confidencial por parte de los*

empleados y proveedores de servicios externos, se tomarán las siguientes medidas.

6.2.1 Empleados nuevos

Durante el proceso de incorporación, el personal de Recursos Humanos deberá:

- *Proporcionar a todos los empleados nuevos acceso a la **Guía para empleados sobre seguridad cibernética** y asegurarse de que todos reconozcan formalmente que han recibido, leído y cumplirán con los todos los requisitos en este documento que se aplican a sus áreas de responsabilidad.*

- *Asegurarse de que todos los empleados completen las actividades de capacitación y concienciación sobre ciberseguridad, según su disponibilidad.*

6.2.2 Empleados existentes

- *Al menos una vez al año, todos los empleados que hayan estado laborando por más de doce (12) meses, deberán completar una sesión anual de capacitación y concientización sobre ciberseguridad y reconocer formalmente la finalización de estos requisitos anuales.*

7 Responsabilidades

7.4 Puerto Rico Innovation and Technology Service (PRITS)

Dentro de PRITS, la Oficina del Principal de Oficial de Ciberseguridad del Gobierno será responsable de las siguientes funciones.

7.4.1.9 Asegurarse de que la agencia cuente con materiales de capacitación relevantes y actualizados para la concientización sobre seguridad.

*7.4.1.17 Realizar esfuerzos de capacitación al personal, contratistas y otros usuarios para concientizar e informar sobre seguridad y (i) los sistemas de información que respaldan las operaciones y los activos de la **agencia**, (ii) los riesgos de seguridad cibernética asociados con sus actividades, y (iii) sus responsabilidades en el cumplimiento de las políticas y procedimientos de la agencia desarrollados para reducir estos riesgos.*

Como norma de control interno y como parte de una sana administración pública toda entidad gubernamental deberá garantizar el buen uso, manejo, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación y manipulación. Como parte de ello, las agencias mantendrán al día un programa de concienciación sobre seguridad de información dirigida a todos los usuarios en todos los niveles.

Efectos

La situación comentada podría tener los siguientes efectos:

1. Aumentan el riesgo de pérdida y divulgación no autorizada de la información, y propiciar el uso indebido de los sistemas de información y el acceso no autorizado a los programas o datos del DTOP y la ACT.

2. La falta de conocimiento de las normas de seguridad relacionadas con los sistemas de información ocasiona el incumplimiento de las mismas con los consiguientes efectos adversos en cuanto a la protección de la información y del equipo.

Causa

Las situaciones comentadas se atribuyen a que los directores del Área de Tecnología de Información del DTOP, como de la ACT y la directora ejecutiva del DISCO no cumplieron con su deber de informar a las Oficinas de Recursos Humanos de ambas entidades las necesidades de adiestramientos para los usuarios u operadores, a los fines de mantenerse al día en los conocimientos relacionados con las funciones y en el manejo de la seguridad de los sistemas a su cargo. Además, no había identificado las necesidades de adiestramiento y la seguridad de la información para los empleados del DTOP y la ACT.

Además, la Directora de Recursos Humanos del DTOP no mantenía un programa continuo de adiestramientos al personal que incluyera las orientaciones sobre las normas, los reglamentos y los procedimientos relacionados con los sistemas de información computadorizados.

Asimismo, no había identificado las necesidades de adiestramiento de los usuarios sobre el uso de los sistemas computadorizados a los fines de planificar y coordinar adiestramientos y orientaciones sobre la seguridad de la información para los empleados del DTOP.

Ver recomendaciones 1 y 5

Hallazgo 15- Reglamentación de los sistemas de información sin actualizar

Situación

Al 28 de febrero de 2023, el DTOP no había actualizado la siguiente reglamentación relacionada a los sistemas de información para atemperarlos con los cambios administrativos, operacionales y organizacionales:

a. *Reglamento Interno sobre el uso de los sistemas de información del Departamento de Transportación y Obras Públicas Número RI-OP-2003-01,* aprobado el 28 de julio de 2004.

b. Reglamento Número 8683 *Reglamento de Acceso al Sistema DAVID+*, aprobado el 30 de diciembre de 2015.

c. Reglamento Núm. 7495, sobre *Normas Sobre el Uso y Control de las Computadoras y sus Programas* de la Autoridad de Carreteras, aprobado el 22 de abril de 2008.

El Reglamento Número 8683 lleva vigente 7 años y el Reglamento Núm. 7495 lleva vigente 14 años, por lo que sus revisiones se hacen necesarias para asegurarse de contar con los mecanismos de control que permitan realizar los procesos de manera uniforme y correcta y sean atemperados con los cambios ocurridos en todos los componentes operacionales del DTOP y en el Área de Tecnología de Información de la ACT.

Criterio

La situación comentada en el **apartado a.** es contraria al Artículo 7 incisos g y l de la Ley Núm. 15-2017, según enmendada conocida como la *Ley del Inspector General de Puerto Rico* que dispone:

> *g. Llevar a cabo aquellos estudios, exámenes y evaluaciones que se consideren necesarios para medir, mejorar y aumentar la efectividad, la eficiencia y la economía en el funcionamiento de las entidades gubernamentales, así como recomendar la eliminación de disposiciones reglamentarias o reglamentos innecesarios, mejorar el servicio al pueblo y recomendar la eliminación de procedimientos ineficientes e inefectivos.*
>
> *l. Evaluar y realizar recomendaciones sobre la legislación, reglamentos existentes y propuestos relacionados con los programas de operaciones de las entidades gubernamentales.*

Las situaciones comentadas en los **apartados b. y c.** son contrarias a la Sección 2.19 de la Ley Núm. 38-2017, conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*, según enmendada, en la cual se establece lo siguiente:

> *Será deber de todas las agencias revisar cada cinco (5) años sus reglamentos para evaluar si los mismos efectivamente adelantan la política pública de la agencia o de la legislación bajo el cual fue aprobado el reglamento.*

Efecto

Las situaciones comentadas tienen el efecto de lo siguientes:

1. El propiciar que el personal de la agencia no cuente con normas o procedimientos actualizados que les sirvan de guías para realizar sus funciones de forma uniforme, efectiva y eficiente.

2. Dificulta adjudicar responsabilidad en caso de que ocurran errores e irregularidades en dichas operaciones.

3. No se ajustan a las nuevas infraestructuras que se han adoptado.

Causa

La situación comentada pudo ser causada, entre otras cosas, por lo siguiente:

1. Los funcionarios encargados de las áreas mencionadas no se aseguraron de realizar las gestiones para la revisión y actualización de la reglamentación y remisión a la primera autoridad nominadora para su aprobación.

2. Los funcionarios que actuaron como secretarios del DTOP tampoco se lo requirieron.

Ver recomendaciones 1 y 2 q

COMUNICACIÓN GERENCIAL

El borrador de los resultados y hallazgos de este examen se sometieron para comentarios mediante carta del 24 de abril de 2023, a la secretaria del DTOP. La secretaria mediante su asesor legal sometió sus comentarios a los resultados y hallazgos mediante carta recibida el 17 de mayo de 2023, donde estableció, entre otras cosas lo siguiente:

> *Actualmente el DTOP está evaluando cada uno de los hallazgos señalados y nos encontramos laborando en los primeros borradores de las acciones correctivas. Esto con el propósito de atender cada uno de los hallazgos con el fin de cumplir oportunamente con las leyes a las que hace referencia dicho informe y mejorar la ejecución de nuestros servicios a la ciudadanía.*

La OIG está comprometida con velar que las recomendaciones sean debidamente cumplimentadas e implantadas y continuará trabajando con el DTOP en aras de continuar promoviendo una sana administración.

RECOMENDACIONES

Debido a las serias deficiencias de controles que existen en el DTOP y el riesgo de seguridad de la información de los usuarios se requiere que se atiendan de manera urgente las siguientes recomendaciones dentro de los próximos 90 días calendario.

A la secretaria del DTOP

1. Requerir por escrito al director ejecutivo de la ACT cumplir con las **recomendaciones de la 2 y 3** y asegurar su cumplimiento. **[Hallazgos 1 al 8, 10 al 13 y 15]**

Al director ejecutivo de la ACT

2. Impartir instrucciones al director del ATI para que:

    a. Comience el proceso de requisición para la adquisición de los equipos obsoletos, independientemente se concrete la migración del Sistema David+ a *Microsoft Azure: Cloud Computing Services*, según notificado y de mantener la red actual de comunicaciones del *Minilla Data Cente*r. **[Hallazgo 1]**

    b. Preparar y someter al PRITS el Plan estratégico conforme el Artículo 13 *Oficial Principal de Informática de las agencias*, Apartado (a) de la Ley Núm. 75-2019. **[Hallazgo 2]**

    c. Realizar y documentar un análisis de riesgos que considere todos los sistemas de información computadorizados del DTOP y la ACT, según se establece en la Política Núm. ATI-015 de la Carta Circular Núm. 140-16. Utilice como base para la preparación y ejecución de una evaluación de riesgo la *Guide for Conducting Risk Assessments*, promulgada por la NITS (*Final Publication*: https://doi.org/10.6028/NIST.SP.800-30r1). **[Hallazgo 3]**

    d. Una vez promulgado el Plan de Seguridad se le realicen pruebas, por lo menos una vez al año, para medir su eficiencia y efectividad y proceder con su actualización y revisión; y divulgar el mismo a todas los servidores públicos y partes interesadas. **[Hallazgo 3]**

    e. Elaborar un plan de continuidad de negocio (planes de contingencia y planes de recuperación) que permitan garantizar la operación de los sistemas de información y los servicios de comunicación del DTOP, a fin de facilitar la continuidad del servicio público que ofrece esta entidad. **[Hallazgo 4]**

    f. Actualizar el Plan de Contingencia aprobado el 18 de junio de 2009, e incluir todos los aspectos mencionados en la situación del **Hallazgo 4**.

    g. Observar lo establecido en la *Política ATI-015*, *Programa de Continuidad Gubernamental,* de forma tal, que se mantenga una estructura de continuidad adecuada

en las operaciones computadorizadas del DTOP, específicamente con el Sistema DAVID+ y realizar pruebas o simulacros, por lo menos una vez al año, para garantizar la efectividad y funcionabilidad del Plan. **[Hallazgo 4]**

h. Formalizar un acuerdo por escrito con un centro alterno que acepte la utilización de sus equipos en caso de una contingencia, desastres o emergencias en el DTOP y la ACT, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra el ATI de la ACT y la OSI del DTOP. **[Hallazgo 5**]

i. Identificar alternativas que sean costo-efectivas para preparar y remitir para la aprobación de la secretaria del DTOP lo siguiente:

   1). Un Plan para el Manejo de Incidentes que contenga un procedimiento a seguir y como parte de dicho procedimiento, se debe requerir que se documenten todos los incidentes y se indique cómo se resolvieron, de manera que, cuando estos se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones del DTOP y de la ACT, específicamente con el Sistema DAVID+. **[Hallazgo 6**]

j. Establecer un plan de trabajo para que se organicen el cableado de los equipos de comunicación en el *Minilla Data Center* y en los cuartos de distribución de cableado. **[Hallazgo 8]**

k. Imparta instrucciones al responsable de administrar la seguridad de los sistemas de información de la ACT, para que:

   1) Establezca las medidas y los controles necesarios para corregir las situaciones indicadas en los **Hallazgos 8**. Esto, de manera que se asegure de que los equipos de comunicación de la ACT y el DTOP estén protegidos contra posibles accesos no autorizados, que puedan afectar la confidencialidad de la información y la disponibilidad y el rendimiento de estos equipos. **[Hallazgos 8]**

   2) Prepare un diagrama esquemático de la red de comunicación de la ACT que incluya la interconexión de los equipos (*switches*, entre otros), la descripción del equipo y su configuración básica (modelo, nombre, *IP Address*), y el sistema operativo de las computadoras conectadas a la red. Además, asegurarse de que se mantenga actualizado. **[Hallazgo 11]**

l. Establecer procesos de supervisión para monitorear el cumplimiento del contratista en establecer las medidas de control necesarias para corregir las situaciones relacionadas con cumplimiento con la protección física del *Datacenter Collocation* donde se mantiene el servidor que reside el Sistema DAVID+. **[Hallazgo 10]**

m. Asegurarse que se prepare y mantenga actualizado un diagrama esquemático de la red que considere todos los equipos y todas las conexiones en todas las instalaciones de la ACT y del DTOP. **[Hallazgo 11]**

n. Establecer los controles ambientales necesarios para corregir las situaciones indicadas. Esto, de manera que se asegure de que los equipos computadorizados de la ATC se mantengan en lugares donde estén protegidos contra posibles daños causados por condiciones ambientales que puedan afectar su disponibilidad y rendimiento. **[Hallazgo 12]**

o. Instruir al encargado de la propiedad que cumpla con la Ley Núm. 230 del 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico* y con el Reglamento 11 *Normas Básicas para el Control y Contabilidad de los Activos Fijos*, aprobado el 29 de diciembre de 2005, por el Secretario de Hacienda. **[Hallazgo 13]**

p. Se asegure de que se mantenga un registro de los programas adquiridos por el DTOP y la ACT e instalados en las computadoras del ACT y el DTOP, que contenga, entre otra información, el número de la licencia del programa, el costo de los programas instalados, el nombre del proveedor, el nombre del usuario, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado la descripción de la computadora donde están instalados los mismos y el total de licencias adquiridas. Esto, con el fin de mantener un inventario de los programas adquiridos e instalados y detectar la instalación de programas no autorizados. **[Hallazgo 13]**

q. Revisar y actualizar los reglamentos relacionados con los sistemas de información computadorizados, conforme a lo requerido en la Ley Núm. 38-2017 y asegurarse que los mismos describan los procesos según se realizan, así como la estructura organizacional. **[Hallazgo 15]**

3. Instruir al director de la Oficina de Sistemas de Información del DTOP para que observen y les den un fiel cumplimiento a las disposiciones contenidas en la *Ley de la Puerto Rico Innovation and Technology Service.* **[Hallazgo 7]**

4. Instruir a la directora del DISCO para que:

   a. Establezca procedimientos escritos y aprobados que incluyan, entre otras cosas, una comunicación efectiva entre el área de Recursos Humanos, el área en que labora el empleado y el Área de Sistemas de Información del cese del usuario en sus funciones o la desvinculación con un contratista con acceso al Sistema David+ o de la modificación de las funciones o acuerdos para la acción correspondiente. Además, se

asegure de mantener los procedimientos actualizados, y de que el mismo se divulgue a los funcionarios, empleados y contratistas concernientes. **[Hallazgo 9]**

b. Solicitar de forma inmediata la desactivación de las cuentas de exempleados, y de aquellos que no requieran tener acceso, según las funciones que estos realizan en el Sistema David+. **[Hallazgo 9]**

5. Instruir a la directora de Recursos Humanos del DTOP para que desarrolle y mantenga, en coordinación con el director del ATI de la ACT y el director de la OSI del DTOP, un programa continuo de adiestramientos al personal que incluya las orientaciones sobre las normas y los procedimientos relacionados con los sistemas de información, especialmente con la seguridad en los sistemas de información. **[Hallazgo 14]**

6. Instruir a la Oficina de Auditoría Interna **que permaneció en la ACT** que incluya en su plan de trabajo realizar auditorías a aquellas aplicaciones críticas que le brindan un servicio al pueblo y a otras partes interesadas al menos una vez al año. **[Hallazgo 6]**

CONCLUSIÓN

La evaluación realizada a los documentos, y la información recopilada durante nuestro examen, revelaron los hallazgos y deficiencias de controles según detallados, para los cuales se emiten las correspondientes recomendaciones. Será responsabilidad de la gerencia corregir las deficiencias señaladas para evitar que situaciones como las comentadas en los hallazgos se repitan.

Los hallazgos identificados en el presente informe reflejan serias faltas en los controles y seguridad a los sistemas de información del DTOP, incluyendo aquellos que incluyen data sensitiva sobre los usuarios y residentes de Puerto Rico. Considerando la exposición a ataques cibernéticos que se ha tenido en las agencias gubernamentales por los pasados años, tales riesgos hacen al DTOP una entidad sumamente vulnerable a la extracción no autorizada de data sensitiva de los usuarios de sus sistemas de información.

La Secretaria del DTOP debe solicitar con carácter de urgencia a través de la Oficina de Gerencia y Presupuesto y la *Puerto Rico Innovation and Technology Service (PRITS,* el presupuesto necesario para la adquisición de nuevo equipo de tecnología e información que permita salvaguardar la data sensitiva que se administra de los usuarios y residentes de Puerto Rico y atender las acciones correctivas solicitadas en este informe.

Conforme a lo establecido en el Artículo 17 de la Ley Núm. 15-2017, mencionada, la OIG remite el presente informe a la autoridad nominadora para que tome las medidas correctivas que estime pertinentes ante el incumplimiento de leyes y reglamentos. Deberá remitir a la OIG las acciones tomadas para garantizar el fiel cumplimiento de las leyes y reglamentos aplicables. El incumplimiento de lo requerido podría representar la imposición de acciones correctivas o disciplinarias.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017, antes citada. Será responsabilidad de los funcionarios, empleados o cuerpo rector del gobierno de cada entidad, observar y procurar por que se cumpla cabalmente con la política pública. De la misma manera, establecer los controles y mecanismos adecuados para garantizar su cumplimiento. Será el deber, además, de cada uno de estos y de los demás funcionarios y servidores públicos, el poner en vigor las normas, prácticas y estándares que promulgue la OIG, así como de las recomendaciones, medidas y planes de acción correctiva que surjan de las evaluaciones.

Hoy, 11 de septiembre de 2023, en San Juan, Puerto Rico.

Ivelisse Torres Rivera, CFE, CIG
Inspectora General

Ivelisse Rivera García, CIA, CIGA
Directora del Área de
Pre-Intervención y Exámenes

ANEJO 1

EDIFICIO MINILLAS TORRE SUR

No se mantenían organizados, ni identificados, ni amarrados los cables que se conectaban a los equipos de comunicación mantenidos en el *Minillas Data Center* y en los cuartos de distribución de cableado ubicado en los 18 pisos del edificio.

Foto 1

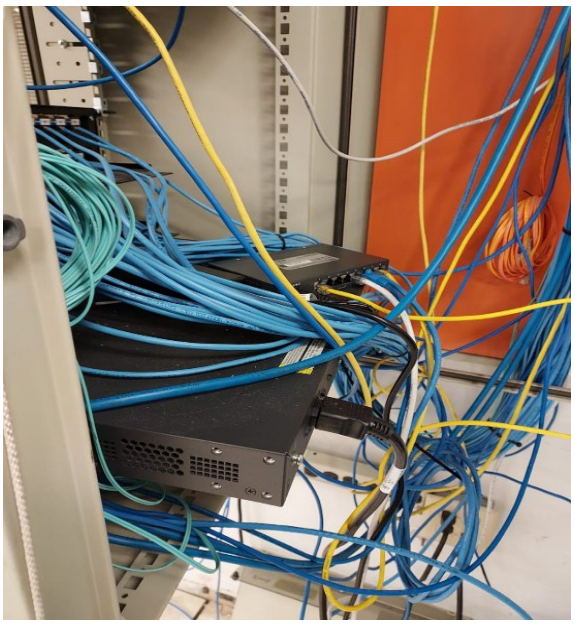


Foto 2

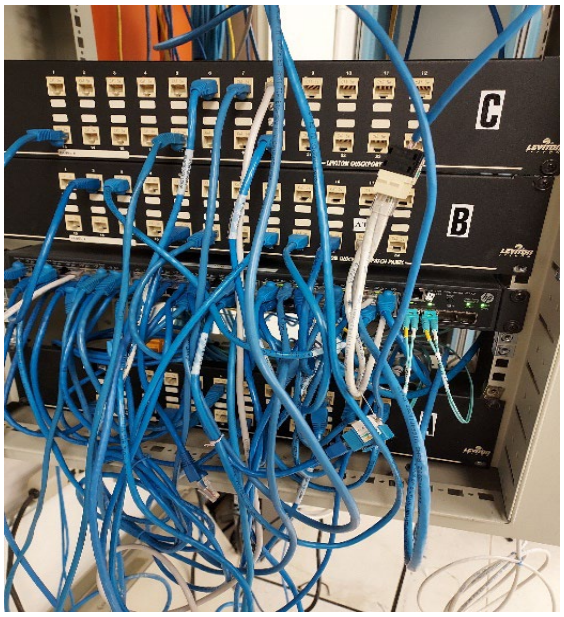


Foto 3

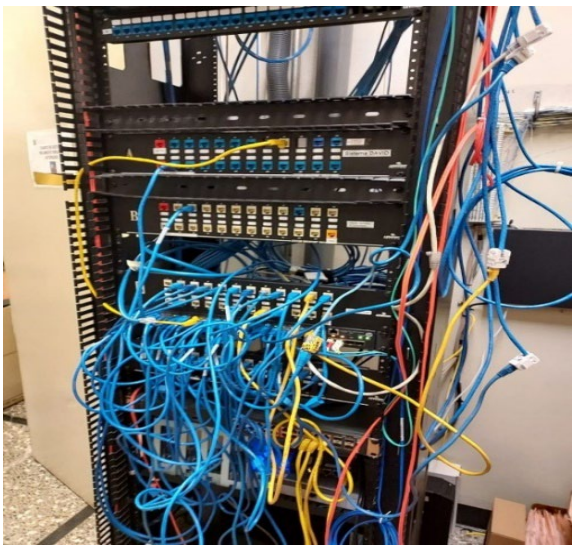


Foto 4

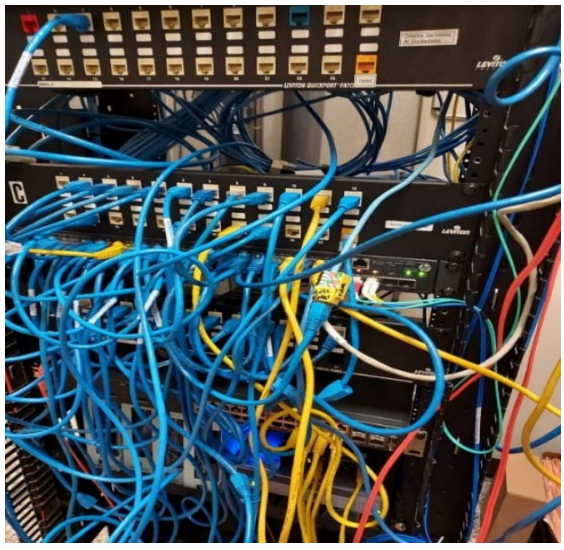


Foto 5

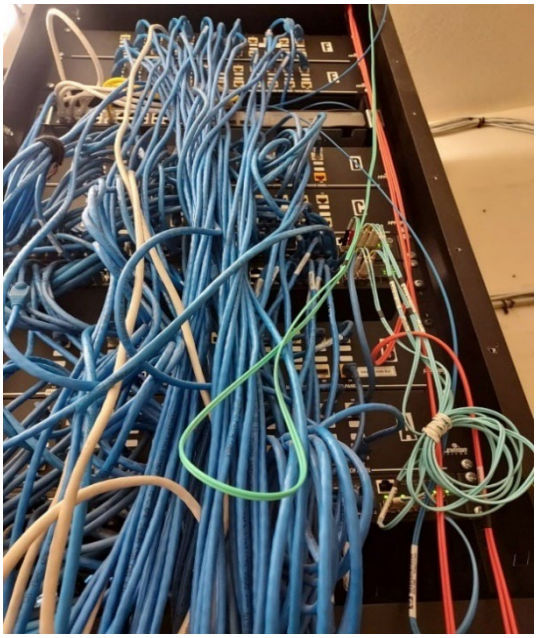


Foto 6

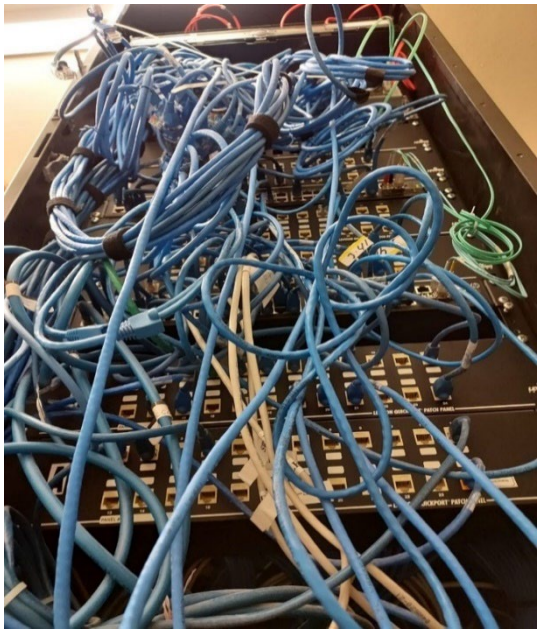


Foto 7

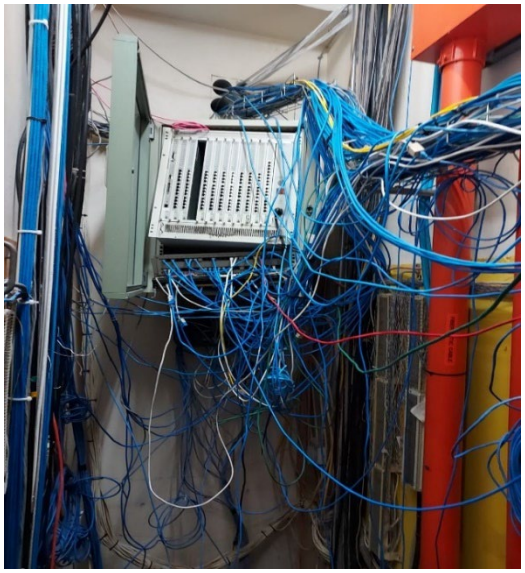
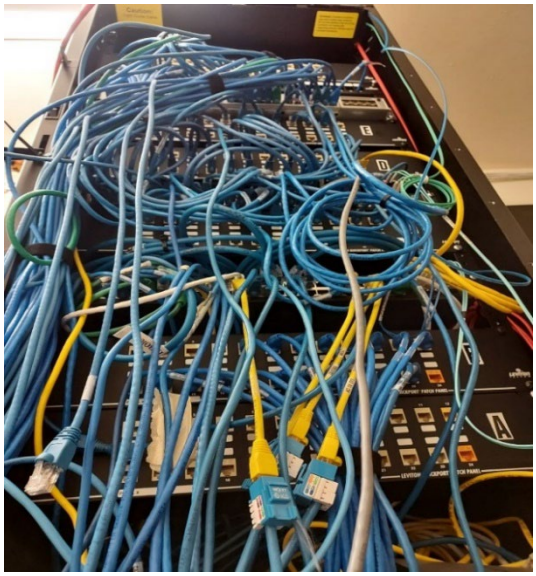


Foto 8



ANEJO 2

CUARTOS DE CABLEADO

Foto 1

INFORMACIÓN GENERAL

Oficina del Inspector General
Gobierno de Puerto Rico

MISIÓN

Ejecutar nuestras funciones de manera objetiva, independiente y oportuna promoviendo mejorar la eficiencia, eficacia e integridad de las entidades bajo nuestra jurisdicción y el servicio público.

VISIÓN

Fomentar una cultura de excelencia mediante la capacitación, observación, fiscalización y desarrollo de sanas prácticas administrativas. Mantener los acuerdos con entidades locales e internacionales para fomentar acciones preventivas en el monitoreo continuo de los fondos del Gobierno de Puerto Rico.

INFORMA

La Oficina del Inspector General tiene el compromiso de promover una sana administración pública. Por lo que, cualquier persona que tenga información sobre un acto irregular o falta de controles internos en las operaciones de la Rama Ejecutiva, puede comunicarse a la OIG a través de:

Línea confidencial: 787-679-7979
Correo electrónico: informa@oig.pr.gov
Página electrónica: www.oig.pr.gov/informa

CONTACTOS

PO Box 191733
San Juan, Puerto Rico
00919-1733

787-679-7997

Ave Arterial Hostos 249
Esquina Chardón Edificio ACAA
Piso 7, San Juan, Puerto Rico

consultas@oig.pr.gov

www.oig.pr.gov