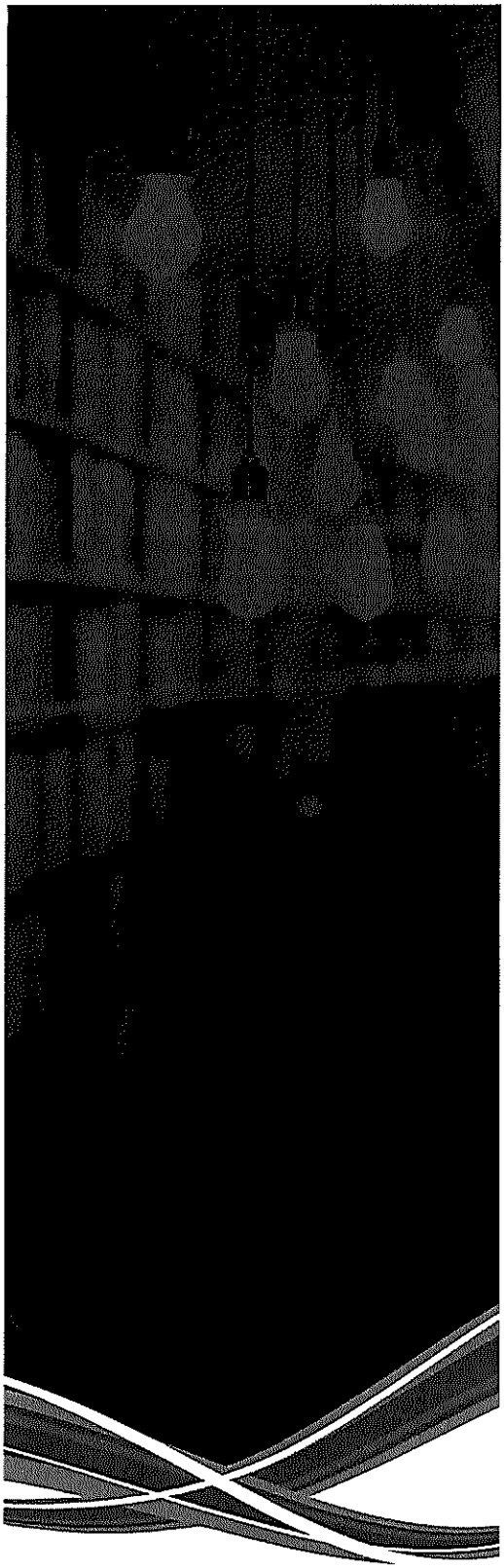

INFORME DE EXAMEN

OIG-E-22-004

JUNTA DE RETIRO
DEL GOBIERNO DE PUERTO RICO

5 de octubre de 2021

OIG

OFICINA DE LA
INSPECTORA GENERAL
GOBIERNO DE PUERTO RICO

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

El 14 de febrero de 2020, la Oficina del Inspector General (OIG), inició un examen de los controles internos de la División de Recaudaciones del Área de Contraloría, y en la Oficina de Tecnología de Información (OTI), de la Junta de Retiro. El examen fue dirigido a evaluar los controles internos en las áreas mencionadas, con el propósito de determinar si ciertas operaciones durante el periodo evaluado se efectuaron de acuerdo con las normas y la reglamentación aplicables; y si los controles establecidos eran efectivos.

La evaluación surge en seguimiento a un incidente informado, sobre un aparente esquema de fraude en el cual se instruía a funcionarios de los departamentos de finanzas de varias entidades de gobierno, por medio de una carta enviada mediante correo electrónico, a redirigir los pagos del *PayGo*, o algún otro pago de remesas del sistema, a un nuevo número de cuenta bancaria. Para realizar este fraude se utilizaron cuentas de correo electrónico de empleados de esa entidad.

Como producto del análisis realizado se identificaron ocho (8), hallazgos relacionados con las operaciones realizadas en la OTI, en lo que concierne a los controles internos establecidos para la administración de la seguridad, el acceso lógico a los sistemas de información, procedimientos adecuados para el manejo de incidentes de seguridad, programa de continuidad del servicio y capacitación al personal. Se identificó, además, un hallazgo relacionado con divulgación de contraseñas. Se emitieron recomendaciones para la atención de los hallazgos que son esbozados en el informe.

La evaluación realizada a los documentos, y la información recopilada durante el examen, demostraron que las operaciones de la OTI, no se realizaron conforme a los estándares de controles internos recomendados. Las deficiencias pudieron haber ocasionado la pérdida de fondos públicos al reflejar vulnerabilidades a los esquemas de fraude por medio de los sistemas de información.

Cabe mencionar, que la investigación correspondiente a identificar los autores del aparente esquema de fraude está a cargo las autoridades estatales y federales.

Conforme a lo establecido en el Artículo 17, de la Ley Núm. 15-2017, *supra*, la OIG remite el presente informe a la autoridad nominadora para que tome las medidas correctivas que estime pertinentes ante el incumplimiento de procedimientos internos, por parte de sus empleados 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 los más óptimos niveles 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 usted conocer sobre actos que podrían poner el 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 o a través del correo electrónico informa@oig.pr.gov.

El presente informe se hace público conforme con lo establecido en la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (Ley Núm. 15-2017); el Artículo 1.9 del Reglamento Núm. 9135, titulado como *Reglamento sobre Asuntos Programáticos de la Oficina del Inspector General*; y el Artículo 1.5 del Reglamento Núm. 9136, titulado como *Reglamento para la Publicación de Informes y Documentos Públicos Rutinarios de la Oficina del Inspector General de Puerto Rico*.

INFORMACIÓN SOBRE LA ENTIDAD EXAMINADA

Mediante la Ley Núm. 447 de 15 de mayo de 1951, se crea un sistema de retiro y beneficios que se denominará "Sistema de Retiro de los Empleados del Gobierno del Estado Libre Asociado de Puerto Rico" el cual se considerará un fideicomiso. Desde su creación, el sistema ha sido objeto de múltiples cambios, como parte de varias enmiendas a su ley orgánica.

Una de las más recientes enmiendas que ha ocasionado cambios significativos en la estructura y funciones de la agencia a cargo de la administración del Sistema de Retiro, ASR[1], ocurrió con la promulgación de la Ley Núm. 106-2017, según enmendada, conocida como la *Ley para Garantizar el Pago de nuestros Pensionados y Establecer un Nuevo Plan de Aportaciones Definidas para los Servidores Públicos*.

Conforme al Capítulo 4, de la Ley Núm. 106-2017, se creó la Junta de Retiro del Gobierno de Puerto Rico, como un nuevo organismo del Gobierno de Puerto Rico, independiente y separado de otros, el cual estaría integrado por 13 miembros.

Durante el período del examen realizado, la Junta de Retiro aún se encontraba en un proceso de transición. El administrador fue designado como director ejecutivo de la Junta de Retiro. De conformidad con el Artículo 5.1, de la citada Ley, los Administradores de los Sistemas de Retiro continuarán ejerciendo sus funciones, descargando sus deberes y tendrán la obligación de brindarle todo el apoyo necesario a la Junta de Retiro y a la Autoridad de Asesoría Financiera y Agencia Fiscal (AAFAF), durante la implementación de dicha Ley, hasta la fecha en que la AAFAF certifique mediante Resolución de su Junta de Directores que se ha completado la transición ordenada por esta Ley. A partir de esa fecha, todos los poderes, deberes y facultades de los Administradores de los Sistemas de Retiro se transferirán permanentemente a las Entidades Administradoras, al Director Ejecutivo de la Junta de Retiro o la persona que la Junta de Retiro determine. Los Administradores de los Sistema de Retiro, al igual que los empleados de los Sistemas de Retiro, continuarán ejerciendo sus funciones durante el periodo de transición. Para propósitos de este Informe nos referiremos al funcionario principal de la Junta de Retiro, como administrador.

Con la enmienda a la ley, se creó una cuenta bajo la custodia del Departamento de Hacienda, para el pago de las pensiones acumuladas, la cual será mantenida en un fondo de fideicomiso separado de los activos generales y cuentas del Gobierno. Esta funcionará bajo el nombre de

[1] Administración de los Sistemas de Retiro.

"*pay as you go*" (*PayGo*), para el pago de las pensiones acumuladas por los sistemas de retiro, incluyendo el sistema de retiro para la judicatura.

El 27 de junio de 2017, el Departamento de Hacienda y la ASR[2], emitieron en conjunto la Carta Circular Núm. 1300-46-17, en la cual se explica la reforma de los Sistemas de Retiro, la implementación del nuevo Sistema de Retiro *PayGo*, las fechas límites y las cuentas a utilizar para los pagos. En la misma se incluyen los números, ruta y tránsito de las cuentas en las que las entidades gubernamentales[3] deberán enviar los fondos de: (1) el "Cargo de *PayGo*"; (2) las aportaciones individuales; (3) descuentos correspondientes a préstamos con los sistemas de retiro y (4) descuentos correspondientes al seguro por incapacidad.

El 8 de enero de 2019, el administrador de los Sistemas de Retiro, emitió la Carta Circular Núm. 2019-03, a las entidades correspondientes, como *Recordatorio sobre cuentas correctas a utilizar para depositar el cargo PayGo, Aportaciones Individuales, Descuentos de Préstamos y Seguro por Incapacidad.* La misma incluye los números de cuenta anteriormente incluidos en la Carta Circular Núm. 1300-46-17.

Para llevar a cabo sus funciones, la Junta también cuenta, además del administrador, con un subadministrador y con las siguientes unidades: Centro de Orientación; áreas de Servicios al Pensionado, Servicios al Participante, Determinación de Incapacidad y de Préstamos; y las oficinas de Contraloría, de Servicios Administrativos, de Tecnología de Información, de Sistemas y Procedimientos, de Comunicaciones, de Recursos Humanos y Relaciones Laborales, y de Asuntos Legales.

Las unidades objeto de evaluación son las siguientes:

División de Recaudaciones del Área de Contraloría[4]

La División de Recaudaciones del Área de Contraloría está integrada por siete (7) empleados. Estos son: una supervisora, una recaudadora, una coordinadora interagencial de recaudos, tres (3) contadores y un oficinista. Esta división es la encargada de facturar a las agencias, corporaciones y municipios, los pagos del nuevo Sistema de Retiro *PayGo,* y cualquier otra remesa. La División realiza el análisis, cuadre y conciliación de cuentas, envía las cartas circulares, facturas o cualquier otro documento a las referidas entidades de gobierno. Además, carga, balancea y archiva las remeses recibidas y prepara los recibos por los recaudos recibidos, depósitos y cuadre del mismo diariamente, entre otras cosas.

En la citada, Ley 106-2017, se dispuso que la Oficina de Gerencia y Presupuesto realizará los pagos en las cuentas designadas para el *PayGo,* al Departamento de Hacienda. Aunque las gestiones de cobro fueron asignadas a la AAFAF, la Junta de Retiro es la entidad que posee las

[2] La Ley 106-2017, que crea la Junta de Retiro, fue promulgada el 23 de agosto de 2017

[3] Dirigida a los Secretarios de Gobierno, Rama Legislativa, Rama Judicial, Jefes de Agencias, Directores Ejecutivos, Presidentes de Corporaciones Públicas y Alcaldes del Gobierno de Puerto Rico.

[4] Se compone además de las oficinas de Presupuesto y de Inversiones, y las divisiones de Cobros, de Contabilidad, de Intervenciones Fiscales, de Pagaduría y de Recaudaciones

bases de datos de los pensionados, por tal razón, funge como una agencia enlace y continúa realizando las funciones antes mencionadas.

Oficina de Tecnología de Información

La Oficina de Tecnología de Información (OTI) está compuesta por siete (7) empleados: un (1) director interino, cuatro (4) técnicos en sistemas de información, una secretaria y una persona a cargo de sistemas y procedimientos. La OTI se rige por varios procedimientos o guías internas. Esta brinda apoyo tecnológico a todas las áreas y oficinas de la Junta de Retiro. Es responsable de custodiar la información electrónica. Además, ofrece apoyo a usurarios (*help desk*), en el manejo y la administración de los diferentes programas de sistemas de información y de los equipos computarizados y en el desarrollo de las aplicaciones. El director interino de la OTI, es supervisado por el subadministrador de la Junta de Retiro.

BASE LEGAL

El presente informe se emite en virtud de los Artículos 7, 8, 9, 16 y 17 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.

OBJETIVOS

Los objetivos del examen realizado en la División de Recaudaciones del Área de Contraloría y en la OTI incluyeron, entre otras, las siguientes operaciones:

De las operaciones realizadas por el Área de Contraloría y la División de Recaudaciones se evaluó el cumplimiento con:

- Delineación e implementación de normas o cartas circulares para la facturación y pago del nuevo sistema de retiro *PayGo*.
- Notificación a las entidades gubernamentales de la implementación de los procesos del *PayGo*.
- Designación previa de un personal para efectuar el proceso de facturación del *PayGo*, o consulta ante cualquier eventualidad.
- Las leyes, reglamentos, procedimientos, políticas o medidas existentes para salvaguardar la confidencialidad de la información sensitiva.
- Medidas inmediatas de mitigación tomadas cuando se detectó el incidente en enero de 2020, entre éstas, comunicación a la gerencia, a las entidades gubernamentales correspondientes y a entidades de ley y orden.

En la OTI se evaluó entre otras cosas, lo siguiente:

- La implementación de controles de acceso y protección de los recursos, que garanticen la confidencialidad, integridad y disponibilidad de la información.

- Establecimiento de las políticas y procedimientos necesarios en el uso adecuado, efectivo y seguro de los sistemas de información.
- Procedimientos de manejo de incidentes de seguridad en los sistemas de información.
- La existencia de un programa de continuidad de operaciones completo, actualizado y funcional.
- Cumplimiento con planes de capacitación y concienciación periódica a usuarios regulares y al personal de tecnología, sobre seguridad y uso apropiado de los sistemas de información.

Las regulaciones aplicables durante el período de examen son las siguientes:

1. Ley Núm. 447 de 15 de mayo de 1951, según enmendada, conocida como *Sistema de Retiro de los Empleados del Gobierno del Estado Libre Asociado de Puerto Rico.*
2. Ley Núm. 106-2017, según enmendada, conocida como *Ley para Garantizar el Pago a Nuestros Pensionados y Establecer un Nuevo Plan de Aportaciones Definidas para los Servidores Públicos.*
3. Carta Circular Núm. 2019-03 – *Recordatorio sobre cuentas correctas a utilizar para depositar el cargo PayGo, Aportaciones Individuales, Descuentos de Préstamos y Seguro por Incapacidad*, emitida el 8 de enero de 2019, por el administrador de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura.
4. Carta Circular Núm. 1300-46-17 – *Implementación del Sistema de Retiro PayGo*, emitida el 27 de junio de 2017, por el secretario de Hacienda y el administrador de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura.
5. 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*, aprobada el 7 de noviembre de 2016 por el director de la Oficina de Gerencia y Presupuesto.

ALCANCE Y METODOLOGÍA DEL EXAMEN

El examen cubrió el período de 1 de noviembre de 2019 al 29 de febrero de 2020. En algunos aspectos se examinaron transacciones de fechas anteriores y posteriores. Se efectuaron pruebas que se consideraron necesarias de acuerdo a las circunstancias. Para realizar la evaluación se utilizaron las siguientes metodologías:

1. Examen y análisis de documentos generados por la unidad evaluada o por fuentes externas.
2. Estudio de leyes, reglamentos, manuales, procedimientos y estándares aplicables.
3. Entrevistas a los directivos de la agencia y a personal de las áreas evaluadas.

4. Observar y verificar las medidas de seguridad implementadas en los sistemas computarizados posteriores al ciberataque detectado en enero de 2020
5. Corroborar las acciones tomadas por la gerencia posterior al incidente.

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

HALLAZGOS

A continuación, detallamos los hallazgos relacionados con las situaciones detectadas durante el transcurso del presente examen.

Hallazgo 1 – Incumplimientos con un programa de continuidad gubernamental

Situación

La continuidad operacional es uno de los conceptos más importantes de la seguridad informática. Las entidades gubernamentales deben establecer una estructura organizacional de continuidad en todas las funciones y procesos críticos ante la eventualidad de una contingencia o desastre. La continuidad asegura que los recursos necesarios para mantener la entidad en funcionamiento seguirán estando disponibles para el personal y los sistemas que dependen de ellos, hasta que se reanuden las operaciones normales.

El examen al cumplimiento de la Junta de Retiro del Gobierno de Puerto Rico (Junta de Retiro)[5] con un programa de continuidad gubernamental reveló lo siguiente:

a. La Junta de Retiro no contaba con un Plan de Continuidad de Operaciones. En su lugar, el director interino de la OTI proveyó un documento titulado *ISO 27001 Security, Roles and Responsibilities for Contingency Planning, Version July 2008,* el cual consiste en unas guías para elaborar el referido plan.

b. A la fecha de finalizar el examen, la Junta de Retiro no había atemperado su Análisis de Riesgos, su Plan de Recuperación de Desastres y su Plan de Manejo de Incidentes, a sus facilidades, infraestructura, cambios tecnológicos, así como del personal responsable de la elaboración y ejecución de los mismos. El Análisis de Riesgo y el Plan de Manejo de Incidentes provistos por la Junta de Retiro tenían fecha de revisión en noviembre de 2015, mientras que el Plan de Recuperación de Desastres fue revisado en septiembre de 2016. Posterior a ese período ocurrieron cambios significativos en la infraestructura. Debido a los efectos del Huracán María en el año 2017, las facilidades, que estaban ubicadas en la Avenida Ponce de León #437 en Hato Rey fueron relocalizadas en el Centro Gubernamental Minillas en la Torre Norte en Santurce. Por otro lado, gran parte del

[5] Antes conocido como la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura.

personal que se identifica como responsable de ejecutar los planes de manejo de incidentes y de recuperación de desastres, ya no laboran en la entidad.

c. En certificación emitida el 13 de noviembre de 2020, por el subadministrador de la Junta de Retiro y el director de la OTI, estos afirman que no se han realizado pruebas de restablecimientos de las operaciones en el centro de recuperación de desastres.

Criterio

Las situaciones comentadas se apartan de lo establecido en la Política ATI-015, Programa de Continuidad Gubernamental, de la Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales, aprobada el 7 de noviembre de 2016, por el director de la Oficina de Gerencia y Presupuesto, que establece, entre otras cosas, que las agencias deberán cumplir con lo siguiente:

B. Estructura de Continuidad

1. Es requerido que cada agencia 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 por el desarrollo de todas las actividades y ejecución del programa de continuidad de la agencia.

C. Análisis de Riesgos – Risk Analysis (RA)

1. Todas las agencias deben realizar un 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.

D. Plan de Recuperación de Desastres – Disaster Recovery Plan (DRP)

1. Todas las agencias deben tener implantado, ejercitado y probado su Plan de Recuperación de Desastres. El Plan de Recuperación de Desastres será actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

E. Plan de Continuidad Gubernamental – Business Continuity Plan (BCP)

1. Todas las agencias deben tener implantado, ejercitado y probado su Plan de Continuidad Gubernamental. El Plan de Continuidad será actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

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.*

3. *El Plan de Continuidad Gubernamental deberá incluir los requerimientos mínimos de operación de cada una de las unidades de la agencia.*

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.*

H. Programa de Pruebas y Ejercicios

El Programa de Pruebas y Ejercicios describe el diseño, desarrollo, ejecución, evaluación y validación de la funcionalidad de las actividades y procedimientos de mitigación, respuesta, recuperación, reanudación y de restauración para todas las funciones y procesos críticas de negocios de la Agencia.

Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. *Toda Agencia deberá realizar al menos un ejercicio y una prueba anualmente para todas sus unidades simulando escenarios de desastre o interrupción del negocio para garantizar que su Plan de Continuidad de Negocios puede ser implementado en situaciones reales de emergencia y desastres.*

2. *Cada Agencia deberá documentar todos los ejercicios y pruebas de continuidad de los diferentes grupos de continuidad.*

3. *Se elabore y se implante el Programa de Pruebas y Ejercicios en base a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).*

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.

O. Manejo de Cambios

La agencia es responsable de diseñar procedimientos que permitan que los cambios a los procedimientos de continuidad sean realizados y documentados y que esta documentación a su vez sea asegurada.

Efecto

Las situaciones comentadas tienen el *efecto* de lo siguiente:

1. Impiden que la entidad pueda estimar el impacto que los elementos de riesgos tendrían en las áreas y los sistemas críticos de ésta, y considerar cómo protegerlos para reducir los riesgos de daños materiales, y de pérdida de la información y los sistemas críticos de esta.

2. Impiden que no se puedan efectuar las tareas de recuperación de las operaciones con prontitud por la falta de un plan que establezca los roles de las tareas a realizar previo al incidente.

3. Propician la improvisación, la duplicidad de esfuerzo y tiempo y que, en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno.

4. Aumentan el riesgo de incurrir en gastos excesivos e innecesarios de recursos y de interrupciones prolongadas de los servicios ofrecidos a los usuarios.

Causa

Las situaciones comentadas se deben a que la gerencia no había cumplido con su responsabilidad, de promulgar directrices sobre la creación de un Plan de Continuidad. Tampoco había tomado las medidas necesarias para que se actualizarán de forma continua, el Análisis de Riesgo, el Plan de Recuperación de Desastres y el Plan de Manejo de Incidentes. Por su parte, los directores en funciones de la OTI no cumplieron con su deber de asegurarse que exista un Plan de Recuperación actualizado y probado para asegurarse que esté listo y operacional.

Comunicación Gerencial

Estas situaciones fueron informadas al administrador de la Junta de Retiro mediante comunicación del 8 de marzo de 2021. El 17 de marzo de 2021, recibimos sus comentarios sobre ésta y otras situaciones informadas.

Como respuesta a la situación comentada en el **apartado a**, el administrador indicó, entre otras cosas, lo siguiente:

> ... *Estamos haciendo los trámites pertinentes para actualizar toda la documentación concerniente a los planes, políticas, reglamentos y procedimientos en el área de Tecnología, incluyendo el BCP y DRP; de igual forma el personal responsable para cada área.*
>
> ... *Nuestra infraestructura actual, nos permite un restablecimiento en varias horas de nuestras aplicaciones críticas. La pérdida de datos e información, se podrían estimar en varias horas, lo cual es aceptable ante cualquier recuperación de un desastre.*
>
> ... *El que no tengamos un plan actualizado, no significa necesariamente, que nuestro tiempo de recuperación sea pernicioso y en contraposición al restablecimiento rápido y seguro de nuestros sistemas.*
>
> ... *Definitivamente la documentación y actualización de los planes nos ofrece un mejor control de recuperación, pero se debe hacer la salvedad, de que las*

personas responsables de los sistemas, tienen el conocimiento, experiencia y destrezas para llevar a cabo estos procesos.

Con respecto a la situación comentada en el **apartado b,** el administrador contestó lo siguiente:

> ... *Nuestro DRC (Disaster Recovery Center), está localizado en Azure en la nube de Microsoft. No se han realizados las pruebas de restablecimiento de los sistemas. No obstante, tenemos todos nuestros servidores virtuales y bases de datos seguros en Azure, desde donde hemos recuperado servidores e información de uso diario.*
>
> ... *En el pasado, y como parte del plan de trabajo, los asuntos antes indicados se trabajarán con el apoyo de la Puerto Rico Innovation and Technology Service (PRITS), y la normativa aplicable bajo la Ley Núm. 75-2019.*

En cuanto a la situación incluida en el **apartado c,** los comentarios del administrador fueron los siguientes:

> ... *Las pruebas se realizaban anualmente, hasta que fueron interrumpidas por el paso del Huracán María, ya que como se menciona en este informe, hubo que relocalizar las operaciones de la Agencia a otro edificio, incluyendo el Centro de Cómputos. Estas pruebas se reanudarán tan pronto se finalice el traslado completo del personal a las nuevas facilidades...*
>
> ... *Tenemos el equipo necesario para recuperar los sistemas críticos, sin necesidad de invertir en otros recursos o tecnología.*

Determinación de la OIG

Se consideraron las alegaciones del administrador de la Junta de Retiro, y se determinó que el **Hallazgo** prevalece.

Ver las recomendaciones 1 y 2.a al d.

Hallazgo 2 – Falta de implementación de funciones básicas de seguridad incluidas en *Microsoft 365*

Situación

La aplicación *Microsoft Office 365* provee funciones o herramientas de protección que, como parte complementaria de otras medidas, pueden reducir o prevenir incidentes de seguridad en los sistemas. Entre estas herramientas se encuentran la autenticación de 2 factores y el cifrado[6] de datos; funciones básicas de seguridad que forman parte de la licencia de Office 365 E3 (Azure.

[6] Cifrado - Procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

Este tipo de licencia es el estándar en las agencias de gobierno, conforme a lo establecido por la Oficina de Gerencia y Presupuesto.

El resultado de las investigaciones forenses realizadas por compañías externas reveló, que, para perpetrar el ataque cibernético detectado en enero de 2020, el atacante[7] pudo acceder y controlar el usuario y contraseña de una cuenta con privilegios administrativos en el entorno de *Office 365*, perteneciente al entonces[8] director de la OTI, y, en combinación con la suplantación de correos electrónicos de otras cuentas de usuarios regulares de la Junta de Retiro, perpetrar el fraude en otras agencias. En la cuenta de administrador global del exdirector de la OTI se detectaron dos autenticaciones diferentes clasificadas como de alto riesgo. Una correspondía a un *IP5*[9] geolocalizado en Nigeria y la otra a un *IP* geolocalizado en Texas.

Posterior al referido incidente, el entonces director de la OTI implementó la autenticación de 2 factores[10] para todas las cuentas de administradores globales o cuentas privilegiadas, y para todos los usuarios cuyas cuentas de correo electrónico fueron afectadas en el referido ataque cibernético. Además, orientó al personal del Área de Contraloría, sobre el cifrado de mensajes de correo electrónico.

Criterio

La situación comentada es contraria a lo establecido en la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos, Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales,* según revisada al 7 de noviembre de 2016. La misma dispone en su *Política ATI-003 Seguridad de los Sistemas de Información*, apartado *J. Internet*, entre otras cosas, lo siguiente:

> *... 4. Si se determina que hay datos sensitivos pasando a través de redes que no son seguras (como internet o redes inalámbricas) se deberá tener los controles necesarios para garantizar la confidencialidad, como por ejemplo el uso de cifrado.*

Además, en la *Política ATI-008 Usos de Sistemas de información, de la Internet y del Correo Electrónico* de la referida Carta Circular, se establece, bajo las *Normas aplicables al uso de correo electrónico*, entre otras cosas, que:

---

[7] A la fecha de este informe el Buró Federal de Investigaciones (FBI, por sus siglas en inglés) no había informado a la Junta de Retiro sobre la identificación del o los perpetradores o sobre el resultado de la investigación.

[8] Director de la OTI desde el 1 de junio de 2017 hasta el 19 de febrero de 2020.

[9] La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo que utilice el protocolo de Internet o, que corresponde al nivel de red del modelo TCP/IP.

[10] Envío de códigos al teléfono celular del usuario

...4. Las entidades gubernamentales deberán establecer claramente una norma con relación a enviar por medio de correo electrónico documentos que contengan información confidencial de la agencia o que contengan información en los cuales se cometen asuntos internos de la agencia que no deben ser divulgados conforme a las normas que rigen la conducta de los empleados. De ser necesario enviar tal información sensitiva la misma deberá ser cifrada (encrypted) para evitar su divulgación...

Efecto

La falta de implementación de medidas de seguridad adecuadas coloca a la agencia en una posición de vulnerabilidad de recibir ataques cibernéticos. Además, propicia que personas no autorizadas puedan tener acceso a información privilegiada y confidencial que maneja la Junta de Retiro.

Causa

El entonces director de la OTI, quien además estaba a cargo de la seguridad de los sistemas, no cumplió con su responsabilidad de implementar y configurar las funciones básicas de seguridad que provee *Microsoft 365,* necesarias y complementarias en la prevención de accesos no autorizados, alteración, divulgación o daños a los sistemas de información.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> *El incidente ocurrido, al cual se hace mención, se tomó acción correctiva, con la implementación del MFA (Multi-Factor Authenticaion), a las cuentas "Global Admin" y a los usuarios involucrados en dicho incidente. Al día de hoy, todos los empleados, sin excepción, tienen habilitada esta herramienta en sus cuentas; además de otras acciones conducentes a mejorar y proteger la seguridad de nuestras aplicaciones de Office 365.*
>
> *... De igual forma, se configuró y condicionó el envío a través de correo electrónico, de información sensitiva, por ejemplo, los documentos que contengan número de seguro social, en donde dicho correo electrónico debe ser cifrado para que ocurra su transmisión.*
>
> *La investigación llevada a cabo por Microsoft, redundó en una serie de recomendaciones, las cuales se han ido implementando; entre ellas, la adquisición de las licencias Azure AD P2, la cual brinda una protección de seguridad, manejada por inteligencia artificial, basada en comportamiento, frecuencias y tendencias. Esta Agencia (Junta de Retiro), es la única que tiene este tipo de licencia en el Gobierno.*

Determinación de la OIG

Reconocemos las medidas tomadas por la gerencia, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que la situación existía al momento en que ocurrió el incidente, y esta falta de medidas de seguridad fue un factor determinante en el ciberataque detectado en enero de 2020.

Ver las recomendaciones 1 y 3.a y b.

Hallazgo 3 – Falta de un plan de manejo de incidentes de seguridad en los sistemas de información

Situación

Una de las mejores herramientas de seguridad en los sistemas de información es la prevención. Un plan de manejo de incidentes es parte esencial de este proceso. Este comienza con el monitoreo constantemente y examen periódico de los registros de seguridad provistos por los sistemas operativos, servidores y en la red, para para conocer las posibles violaciones de seguridad que pudieran ocurrir. Una vez detectado el problema, se debe investigar para determinar su causa, tomar prontamente las medidas preventivas y correctivas necesarias y documentar cada paso de la respuesta para futuras referencias. Las medidas de seguridad y los procesos deben actualizarse, ajustarse y comunicarse al personal correspondiente, para evitar que el incidente se repita.

El examen realizado reveló, que la OTI, no contaba con un plan de manejo de incidentes de sistemas de información en el que se detallaran los procesos de monitoreo, detección, investigación, respuesta y registro de incidentes de seguridad. Los directores en funciones de la OTI, aparte de todas las funciones y responsabilidades inherentes a ese puesto, estaban a cargo de la administración de redes y de la seguridad de los sistemas de información. Estos eran responsables de recibir y revisar notificaciones o alertas sobre aparentes amenazas en los sistemas. No existe un registro en el que se documentaran los incidentes detectados, investigados y las medidas tomadas.

El director interino de la OTI manifestó, en entrevista con los auditores, que no cuenta con el tiempo suficiente para analizar e investigar todas estas alertas. Que debido a las múltiples responsabilidades a su cargo solicitó a la administración la asignación de asistencia en otras labores. No obstante, los puestos en la OTI son clasificados como unionados, por lo que sus funciones están limitadas a las establecidas en las descripciones de deberes.

Criterio

La situación comentada es contraria a la *Política ATI-003, Seguridad de los Sistemas de Información* de la Carta Circular 140-16 que establece, entre otras cosas, lo siguiente:

> *E. Controles Generales*

...7. Deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

F. Manejo de Incidentes

1. *Las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluyendo límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta.*

2. *Todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.*

Por otro lado, en la *Política Núm. ATI-014 Manejo de Firewalls*, de la referida Carta Circular se indica, entre otras cosas, que debido a que el personal de sistemas de información está demasiado ocupado trabajando con asuntos de mantenimiento y soporte de los sistemas informativos, y la seguridad es un tema sumamente complejo y sensitivo, en muchas ocasiones se requiere que exista un oficial o especialista en seguridad informática o sus equivalentes.

Efecto

Las situaciones antes señaladas dificultan el cumplimiento con mantener un sistema de información seguro, pues no se tiene constancia de, entre otras cosas:

- El tipo, frecuencia e impacto de los incidentes detectados
- Qué acciones evitarán que el incidente vuelva a ocurrir
- Qué medidas preventivas deben reforzarse
- Cómo mejorar la supervisión del sistema
- Cómo se puede minimizar el tiempo de inactividad durante las fases de contención, erradicación y recuperación
- Cómo puede la gerencia minimizar el impacto
- Mantener récords de las violaciones de seguridad con detalle suficiente para ser usados en revisiones y/o acciones disciplinarias.

Un ejemplo del efecto de la falta de mantenimiento de récords de incidentes de seguridad es, un incidente relatado por una empleada de la División de Recaudaciones, ocurrido aproximadamente a finales del año 2018. La empleada relató que personal de varias agencias gubernamentales le comunicó que estaba recibiendo correos electrónicos desde su cuenta, los que no fueron enviados y tampoco preparados por ella. Este incidente fue atendido por el entonces director de la OTI, no obstante, el actual director interino de la OTI indicó que desconocía sobre el mismo. Es importante señalar, que a esa empleada fue a quien se le suplantó su cuenta de correo electrónico en el incidente detectado en enero de 2020, mediante el cual se enviaron mensajes fraudulentos a las

agencias gubernamentales en los cuales se les informaba que debían depositar los pagos de remesas a un nuevo número de cuenta bancaria.

Causa

La situación comentada se atribuye en parte, a la multiplicidad de tareas y funciones que realiza el director de la OTI. No se había designado una persona responsable exclusivamente del manejo de la seguridad en los sistemas, tarea que necesita contante dedicación para evitar o mitigar los riesgos de ataques cibernéticos.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> ... *Estamos en el proceso de integrar a un Oficial de Seguridad para que ejerza las funciones y el monitoreo de protección de los sistemas y la seguridad de la red.*
>
> ... *Necesitamos una documentación más efectiva de los incidentes y controles de seguridad, sin embargo, los mismos se han atendido diligentemente. Tomaremos acción al respecto, por lo que estamos haciendo las gestiones para integrar en nuestra oficina de tecnología un Oficial de Seguridad.*

Determinación de la OIG

Se sostiene el hallazgo. El administrador reconoció la necesidad de integrar un oficial de seguridad responsable de, entre otras cosas, el monitoreo y documentación de los incidentes de seguridad.

Ver las recomendaciones 1 y 2.e.

Hallazgo 4 – Falta de un diagrama esquemático de la red

Situación

Las entidades gubernamentales deben 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 eficiente de los servicios. El diseño de esta red debe estar documentado con diagramas esquemáticos que permitan identificar y documentar los dispositivos utilizados para acceder a la misma, las vías de telecomunicaciones y los usuarios de esta, entre otros. Esto, con el propósito de identificar los puntos de acceso a los recursos de la red y controlarlos. Además, el diagrama esquemático debe mantenerse actualizado.

En entrevista del 13 de julio de 2020, con el director interino de la OTI, este indicó que no contaban con un diagrama actualizado de la red. La versión más reciente corresponde a las antiguas facilidades de la Junta de Retiro en Hato Rey, por lo que no se habían contemplado los

correspondientes cambios en las facilidades e infraestructura, además de los cambios en tecnología. A la fecha de la entrevista la Junta de Retiro se encontraba en un proceso de mudanza, del Centro Gubernamental Minillas Torre Norte en Santurce al Edificio Capital Center en Hato Rey.

Criterio

La situación comentada se aparta de la *Política ATI-011, Mejores Prácticas de Infraestructura Tecnológica*, de la Carta Circular 140-16, la cual establece en la sección de Política para el Componente de Red, que el diseño de la red debe estar documentado.

Efecto

La situación comentada impide a la OTI, 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 esta. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Causa

El director en funciones de la OTI no cumplió con su responsabilidad de actualizar el diagrama de la red conforme a los cambios en la infraestructura y facilidades.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> ... *Como menciona el informe de OIG, tenemos un diagrama de la red, el cual no está actualizado debido a los distintos procesos de mudanza que hemos tenido desde el paso del Huracán María...*
>
> ... *Todos los componentes de la red están debidamente rotulados e identificados, lo que nos facilita, detectar algún problema o anomalía que se presente, para poder resolverlo diligentemente.*

Determinación de la OIG

Se sostiene el **Hallazgo**. El administrador reconoció que el diagrama de la red no está actualizado.

Ver las recomendaciones 1 y 3-d.

Hallazgo 5 – Incumplimientos con procedimientos, políticas o estándares del área de sistemas de información

Situación

La mecanización de los procesos en las agencias requiere regular el manejo apropiado de sus recursos informáticos e implementar las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información. Conforme a lo anterior, resulta necesario establecer una defensa sólida mediante el establecimiento de las políticas y procedimientos necesarios en la adquisición y el uso adecuado, efectivo y seguro de los sistemas de información.

El 26 de febrero de 2020, recibimos de la Junta de Retiro, 15 procedimientos, políticas o estándares relacionados con el área de sistemas de información. Uno de los procedimientos se emitió en el año 1984, cinco (5) en el año 2010, siete (7) en el año 2012, uno (1) en el año 2015 y uno (1) en el año 2016.

Del examen realizado a los documentos recibidos se concluyó lo siguiente:

a. Ocho (8) de los procedimientos o estándares no se habían revisado, de manera que se contemplaran los correspondientes cambios en infraestructura o cambios tecnológicos. Uno de los procedimientos hace referencia a otras políticas actualmente derogadas[11]. Los que entendemos deben ser revisados son los siguientes:

(1) *04-84-01– Normas y Procedimientos del Centro de Sistemas Electrónicos de Información* aprobado el 15 de diciembre de 1984[12].

(2) *OT-11-001– Procedimiento para Encender y Apagar los Servidores* aprobado el 16 de agosto de 2010, por el entonces director de la OTI.

(3) *OT-11-E002 – Estándares en la Administración de las Estaciones de Trabajo* aprobado el 14 de noviembre de 2010, por el entonces director de la OTI.

(4) *OT-11-E-003 – Estándares de Nomenclatura de Recursos Tecnológicos* aprobado el 16 de noviembre de 2010, por el entonces director de la OTI.

(5) *OT-13-E-001 – Estándares de Resguardo y Recuperación de Redes* aprobado el 23 de octubre de 2012, por el entonces director de la OTI.

[11] En el procedimiento OT-11-001, se utiliza como referencia la Carta Circular 77-05 de 8 de diciembre de 2004, la cual fue derogada el 7 de noviembre de 2016, por la Carta Circular *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales.*

[12] No indica quién lo aprobó.

(6) *OT-13-E003 – Estándar de Resguardo y Recuperación de la Base de Datos de ASR* aprobado el 26 de noviembre de 2012, por el entonces director de la OTI.

(7) *OT-13-E-004 – Estándar de Procedimientos de Operación para "Shutdown y Startup" de los Servidores de Retiro* aprobado el 29 noviembre 2012, por el entonces director de la OTI.

(8) *Manual Infraestructura y Configuración de la Red* aprobado el 28 de febrero de 2012 por el entonces director de la OTI.

b. La Junta de Retiro tiene en borrador un *Manual de Políticas de Sistemas de Información,* que fue revisado al 30 de septiembre de 2015; no obstante, no había sido aprobado por los funcionarios correspondientes. En nuestra evaluación se determinó que el referido manual incluye políticas de controles internos relacionadas con los sistemas de información y otros procesos, por lo que es meritorio e impostergable su actualización y correspondiente referido a la Junta para su aprobación.

Una situación similar fue comentada en el Informe TI-13-06 del 12 de septiembre de 2012, emitido por la Oficina del Contralor de P.R.

Criterio

La situación comentada es contraria a lo establecido en el Artículo 4-103 inciso (6), de la Ley Núm. 447 de 15 de mayo de 1951, según enmendada, conocida como *Sistema de Retiro de los Empleados del Gobierno del Estado Libre Asociado de Puerto Rico*. El mismo establece que, entre las facultades y deberes del Administrador estará la preparación de reglamentos para la aprobación de la Junta.

Además, la situación comentada es contraria a la *Política Núm. ATI-003, Seguridad en los Sistemas de Información* de la *Carta Circular Núm. 140-16*, en la cual se establece, entre otras cosas, que será responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables que le permitan establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Las políticas y procedimientos de seguridad deberán estar de acuerdo a la legislación y los reglamentos vigentes que apliquen.

Por otro lado, según la Descripción de Puesto del director de Tecnología de Información con fecha de efectividad de 16 de junio de 2017, entre las funciones de ese puesto se encuentran, desarrollar y evaluar los conceptos, mecanismos, reglamentación y procesos que se utilicen en todas las actividades y estructuras de informática de la agencia con el fin de agilizar las operaciones. Además, evaluar las normas y procedimientos internos de la OTI y recomendar modificaciones con el fin de mejorar los servicios que ésta preste.

Efecto

Las situaciones comentadas propician la improvisación y falta de uniformidad en las operaciones. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas. Además, podría exponer al personal, a los equipos y a la información de la agencia a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

Causa

Los directores en funciones de la OTI, no cumplieron con lo establecido en el referido Manual, de mantener actualizadas las políticas, estándares y procedimientos mencionadas. La situación comentada se atribuye, en parte, a la multiplicidad de tareas y funciones que realiza el director interino de la OTI. Por su parte, la gerencia no supervisó adecuadamente estas operaciones de manera que se asignaran los recursos necesarios para revisar y actualizar las políticas, estándares y procedimientos.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> *Estamos conscientes del beneficio y seguridad que proveen las Normas, Procedimientos, Políticas y estándares para una organización; como se menciona en este informe, tenemos redactados y desarrollados todos los documentos relacionados al mantenimiento de los sistemas, no obstante, debemos actualizar los mismos y atemperarlos a las realidades vigentes. Tenemos un plan diseñado para llevar a cabo una actualización completa de todos estos documentos.*

Determinación de la OIG

Se sostiene el **Hallazgo**. El administrador reconoció la situación señalada.

Ver las recomendaciones 1 y 2.f.

Hallazgo 6 – Incumplimiento con controles relacionados a la confidencialidad de contraseñas

Situación

La naturaleza del trabajo que se realiza a través de los sistemas de información requiere que a un empleado se le otorgue acceso, mediante el uso de contraseñas, a los sistemas computarizados. Las contraseñas son una de las herramientas fundamentales de la seguridad de los recursos informáticos; pues se trata de la primera línea de protección para usuarios y administradores de sistemas. La seguridad provista por una contraseña depende de que el usuario mantenga su confidencialidad y por

ningún motivo divulgarla. El personal debe ejercer buenas prácticas para garantizar la seguridad de su contraseña, lo que a su vez garantiza la confidencialidad y seguridad de la información de la entidad en la cual labora.

En entrevista realizada a la supervisora interina de la División de Recaudaciones ésta indicó que, "todo el mundo sabe las contraseñas de los demás" y cuando es necesario utilizarlas se comunica con el empleado para notificarle. Además, la Coordinadora Interagencial de Recaudo indicó, que si necesita ausentarse o está de vacaciones la supervisora interina de la División de Recaudaciones y la recaudadora saben dónde mantiene escrita su contraseña y que de necesitar la misma se comunican con ella para notificarlo.

Criterio

La situación comentada se aparta además de la *Política ATI-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la Carta Circular 140-16 que dispone, entre otras cosas, que cada usuario será individualmente responsable por el manejo adecuado de los códigos de acceso o contraseñas asignadas.

Efecto

Esta situación puede traer como resultado que, en caso de que se realice el uso indebido a través de un acceso de usuario o contraseña, se dificultaría la adjudicación de responsabilidades. Además, esta situación puede generar conflicto en los procesos de auditoría y revisión de accesos.

Causa

Las referidas empleadas incumplieron con los controles establecidos de mantener la confidencialidad de las contraseñas.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> *El uso y disponibilidad de las contraseñas es una acción individual y personal, la Agencia en ningún momento ha promovido compartir ni divulgar las mismas. El comportamiento llevado a cabo por los usuarios mencionados en este informe, no es la norma ni la costumbre de la mayoría de los empleados. Las razones de obrar de esa forma, concerniente a este tema, no es cónsona con las políticas y normas que tenemos para el uso de contraseñas.*

Determinación de la OIG

Consideramos las alegaciones del administrador, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que el señalamiento se adjudica a las empleadas mencionadas.

Ver las recomendaciones 1, 2.g y h.

Hallazgo 7 – Falta de capacitación y adiestramientos para el personal de tecnología y usuarios de los recursos informáticos

Situación

Una de las mejores herramientas de seguridad en los sistemas de información es contar con un personal debidamente adiestrado y con los conocimientos actualizados, ante las nuevas técnicas de ataques, amenazas y vulnerabilidades. La creación de un programa de capacitación y una cultura de concienciación en ciberseguridad es un esfuerzo continuo que requiere el liderazgo de la alta gerencia y el compromiso de todos los usuarios.

El examen del cumplimiento con las medidas de capacitación y adiestramientos relacionados con la seguridad en los sistemas de información, al personal técnico y a los usuarios regulares, reveló lo siguiente:

a. Los directores en funciones de la OTI no habían recibido adiestramientos relacionados con sistemas de información del período del 1 de enero de 2017 al 29 de febrero de 2020, según certificación emitida el 20 de julio de 2020, por la Oficina de Recursos Humanos. Esta información fue corroborada en entrevista realizada el 13 de julio de 2020, al director interino de la OTI quien nos indicó, entre otras cosas, lo siguiente:

    1) No existe un plan de adiestramientos periódicos a los usuarios o al personal de la OTI, sobre seguridad en el uso de los sistemas de información.

    2) Recientemente (luego del ciberataque detectado en enero de 2020), ha tomado varios cursos impartidos por *Microsoft*. Entre ellos un curso de seguridad en *Office 365*, el cual fue gestionado por *Puerto Rico Innovation and Technology Service (PRITS)*.

    3) No ha recibido adiestramientos relacionado a la administración del *firewall*[13]. No obstante, ha estado administrando el mismo por los pasados 5 años y ha adquirido conocimientos para poder manejar las principales funciones del mismo de manera autodidacta.

b. En entrevista a otro técnico de sistemas que labora en la OTI, éste indicó, que durante los últimos años no había recibido adiestramientos de capacitación en sistemas de información, ya sean internos o externos.

c. En entrevistas realizadas a cuatro empleadas de la División de Recaudaciones, éstas manifestaron no haber recibido adiestramientos u orientaciones relacionadas con la

[13] *Firewall* (Servidor de Seguridad de Computadoras y Redes) – Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados.

seguridad en el uso de recursos informáticos antes del ciberataque detectado en enero de 2020. A raíz de ese incidente, el entonces director de la OTI les orientó sobre el cifrado, cuarentena de correos electrónicos, la autenticación multifactor, y notificar y no abrir correos sospechosos.

Criterio

La situación comentada es contraria a la *Política ATI-003, Seguridad de los Sistemas de Información,* de la Carta Circular 140-16 que establece, entre otras cosas, lo siguiente:

H. Adiestramientos

1. *Cada agencia es responsable de proveer adiestramientos al personal para que estén al tanto de los controles de seguridad y los beneficios correspondientes.*

2. *El personal de sistemas de información y telecomunicación deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.*

3. *Se deben proveer mecanismos para capacitar a todos los empleados periódicamente.*

Además, en la *Política ATI-014, Manejo de Firewalls* de la referida Carta Circular se establece, entre otras cosas, que toda agencia debe tener personal capacitado y adiestrado en seguridad y en el manejo de *firewalls*.

Por otro lado, según la Descripción de Puesto del director de Tecnología de Información[14] con fecha de efectividad de 16 de junio de 2017[15], se establece, que entre las funciones de ese puesto se encuentra determinar las necesidades de adiestramientos y capacitación del personal de la OTI.

En la Descripción de Puesto para gerente de servicios técnicos[16] con fecha de efectividad de 1 de septiembre de 2016, indica, que como parte de sus funciones está, planificar y recomendar adiestramientos para el personal bajo su supervisión.

Efecto

Esta situación puede reducir la efectivad y el desempeño del personal de la OTI. Además, la ausencia de capacitación y educación continua expone la información de la Junta de Retiro a riesgos innecesarios relacionados con la seguridad y protección de los sistemas computarizados.

Causa

La situación comentada se atribuye a que los directores en funciones de la OTI no cumplieron con su responsabilidad de procurar que se estableciera un programa de adiestramientos para capacitar

[14] Formulario ASR-RH-056 Rev. junio 15. Descripción de Puesto.
[15] Puesto perteneciente al anterior director de la OTI (desde 16 de junio de 2017 hasta el 19 de febrero de 2020).
[16] Puesto perteneciente al actual director interino de la OTI.

al personal de los sistemas de información. Tampoco cumplieron con educar a los usuarios sobre los procedimientos seguros en el uso de los recursos informáticos. La gerencia tampoco veló por el cumplimiento de estos procesos.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> *Concerniente a los adiestramientos para el personal de la Oficina de Tecnología de Información, éstos han sido tomados, de acuerdo a la función y desempeño de cada empleado. En los últimos 4 años, en la Oficina ha habido una reducción de personal muy significativa; las funciones y manejo de las actividades han sido delegadas y administradas por un reducido número de empleados, éstos han sido adiestrados por otros compañeros, sin embargo, no así, por algún ente externo que expida una certificación. En el caso del Director Interino, este ha indicado que ha tomado varios cursos y adiestramientos de seguridad, sin embargo, no lo había informado a la Oficina de Recursos Humanos de la Agencia.*
>
> *Con relación a los empleados de las demás áreas, éstos han sido notificados y orientados sobre el uso de los sistemas, incluyendo los correos electrónicos. De igual forma, existe una advertencia, la cual se despliega en la pantalla del monitor de todos los usuarios que ingresan a la red, donde se especifica las normas y usos de los sistemas de información.*

Determinación de la OIG

Se consideraron las alegaciones del administrador y se determinó que el **Hallazgo** prevalece. **Ver las recomendaciones 1, 3.e y f.**

Hallazgo 8 – Falta de desactivación de la cuenta de acceso a empleada que cesó funciones

Situación

La desactivación inmediata de la cuenta de acceso de los empleados que cesan o se separan de sus funciones es una de las mejores prácticas para evitar irregularidades en los sistemas computarizados.

Una evaluación realizada sobre el estatus de las cuentas de accesos de 20 empleados que habían cesado sus funciones en la Junta de Retiro durante el período del 1 de enero de 2019 al 24 de

febrero de 2020, reveló, que al 10 de agosto de 2020, no se había desactivado de *Azure Active Directory*[17] la cuenta de acceso de una empleada que se había retirado el 31 de diciembre de 2019.

La Oficina de Recursos Humanos y Relaciones Labores proveyó el formulario ASR-RH-022, *Relevo de Asuntos Pendientes en la Administración* correspondiente a la referida empleada, el cual fue tramitado a varias unidades[18] de la Junta de Retiro. De conformidad con los procedimientos establecidos[19] ante la terminación o conclusión de empleo o contrato, esa oficina notificó a la OTI con no menos de 7 días laborables de antelación a la terminación de empleo. El 19 de diciembre de 2019, el entonces director de la OTI certificó en el mencionado formulario, que a la referida empleada se le canceló el acceso a la información electrónica del Sistema[20].

Criterio

En la *Política Núm. ATI-003, Seguridad en los Sistemas de Información* de la *Carta Circular Núm. 140-16* se establece, entre otras cosas, que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada.

Efecto

Esta situación puede ocasionar que personas no autorizadas accedan y hagan uso indebido de los sistemas por error o deliberadamente. Además, esto provoca que en caso que surjan irregularidades con esta cuenta de acceso, se dificulte la adjudicación de responsabilidades.

Causa

El entonces director de la OTI no cumplió con su responsabilidad y lo establecido en las políticas mencionadas, de desactivar el acceso de la referida empleada, aun cuando certificó que el acceso había sido cancelado.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

---

[17] *Azure Active Directory (Azure AD)* es un servicio de administración de identidades y acceso basado en la nube de *Microsoft* que ayuda a los empleados a iniciar sesión y acceder a recursos externos, como *Microsoft* 365, y recursos internos, como las aplicaciones de la red corporativa y la intranet, junto con todas las aplicaciones en la nube desarrolladas por su propia organización.

[18] Oficina de Asuntos Legales (investigaciones), División de Transporte y Correspondencia (vehículos y licencias), División de Seguridad, Propiedad y Suministros (propiedad), Oficina de Servicios Administrativos (estacionamiento), División de Contabilidad (deudas), División de Adiestramientos y División de Licencias.

[19] Conforme al apartado *C. Terminación o Conclusión de Empleo o Contrato*, del *Estándar OT-11-E001, Estándares de Solicitudes de Servicios y Acceso a las Aplicaciones*, aprobado por el director de la OTI el 10 de noviembre de 2010.

[20] Sistema se refiere a la Administración de los Sistemas de Retiro. Actualmente Junta de Retiro.

La desactivación de las cuentas de empleados que han cesado sus funciones se realiza por conducto de un documento, el cual provee la Oficinas de Recursos Humanos. El caso específico al que se hace mención, no constituye la norma ni el proceder ordinario de OTI (Oficina de Tecnología de Información). Cabe señalar, que el Azure AD, se nutre de la información que reside en el Local AD, por lo que cualquier cuenta que se desactive localmente se reflejará en la nube (Azure AD).

Determinación de la OIG

El **Hallazgo** se sostiene. El administrador reconoció que, aunque no es la norma, la situación ocurrió.

Ver recomendaciones 1, 3.g y h.

Hallazgo 9 – Ausencia de controles que regulen el uso adecuado de recursos

Situación

Es necesario mantener un control adecuado sobre el uso y manejo de recursos en las agencias gubernamentales. El equipo multifuncional (impresora/fotocopiadora/escáner), así como todo aditamento, como son, tóner y papel de impresión, deben utilizarse únicamente para los propósitos que fueron destinados.

En entrevista realizada el 9 de julio de 2020, al director interino de la OTI, nos indicó que no se requería de un código individual por empleado para el uso de los equipos multifuncionales.

Criterio

La situación comentada es contraria al artículo 2(f) de la Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico* que establece, entre otras cosas, que exista un control previo de todas las operaciones del gobierno; que dicho control previo se desarrolle dentro de cada dependencia, entidad corporativa o Cuerpo Legislativo para que así sirva de arma efectiva al jefe de la dependencia, entidad corporativa o Cuerpo Legislativo en el desarrollo del programa o programas cuya dirección se le ha encomendado. Tal control interno funcionará en forma independiente del control previo general que se establezca para todas las operaciones de cada rama de gobierno.

Efecto

Esta situación puede propiciar el uso indebido, o para otros fines que no sean públicos, de los recursos del gobierno sin que se pueda detectar y fijar responsabilidades.

Causa

Se atribuye esta situación a que la gerencia de la ASR no había establecido controles efectivos que garantizaran el uso adecuado de los referidos recursos.

Comunicación Gerencial

En la comunicación del 17 de marzo de 2021, el administrador de la Junta de Retiro, indicó, entre otras cosas, lo siguiente:

> *Entendemos que es una buena práctica asignar un código a cada empleado, para un mejor control. Estamos tomando las acciones pertinentes para activar dichos controles.*

Determinación de la OIG

El **Hallazgo** se sostiene. El administrador reconoció la situacion señalada.

Ver las recomendaciones 1 y 3.i.

COMENTARIO ESPECIAL

Como resultado del examen realizado en la Junta de Retiro, la OIG recomienda a la *Puerto Rico Innovation and Technology Service (PRITS)* que evalúe la viabilidad de establecer la licencia *Azure AD P2*[21] de Microsoft como el estándar en las agencias gubernamentales. **Ver el Hallazgo 2.**

La Ley Núm. 75-2019, conocida como la *ley de la Puerto Rico Innovation and Technology Service (PRITS),* crea esa entidad adscrita a la Oficina del Gobernador con el fin de establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración interagencial efectiva de la innovación y de la infraestructura tecnológica e informática del Gobierno de Puerto Rico, así como desarrollar de forma ordenada e integrada los proyectos tecnológicos puntuales necesarios para promover la integración efectiva de la tecnología a la gestión gubernamental; definir las funciones y las facultades del Principal Ejecutivo de Innovación e Información del Gobierno de Puerto Rico y el Principal Oficial de Tecnología del Gobierno de Puerto Rico.

Conforme al Artículo 5 de la Ley 151-2004, entre las funciones de la PRITS estarán las siguientes:

> ... (h) Incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico, por medio de licenciamientos y adiestramientos globales u otros esquemas ventajosos a nivel gubernamental.

[21] https://azure.microsoft.com/en-us/pricing/details/active-directory/

(i) Desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y los activos gubernamentales.

De otra parte, en el Artículo 6 de la Ley 151-2004 se establece que, entre las facultades de la PRITS estarán las siguientes:

... (h) Podrá servir de ente coordinador de las correspondientes áreas de sistemas de información de las diferentes agencias e instrumentalidades de manera que se puedan incorporar efectivamente las mejores prácticas del sector tecnológico.

(i) Podrá agenciar proyectos de tecnología con impacto interagencial.

Ver la recomendación 4.

COMUNICACIÓN GERENCIAL

El 8 de marzo de 2021, se envió a la Junta de Retiro una carta a la gerencia con las 9 situaciones determinadas en dicho examen. El 17 de marzo de 2021, el administrador emitió sus comentarios aceptando 5 de las situaciones (hallazgos 1, 3, 4, 5 y 9). Cuatro de las situaciones no fueron aceptadas (hallazgos 2, 6, 7 y 8).

Se evaluaron cuidadosamente los comentarios sometidos por la gerencia y los mismos fueron considerados al redactar este Informe.

La OIG está comprometida con velar que las recomendaciones sean cumplimentadas e implantadas. Se continuará trabajando con la Junta de Retiro para promover el establecimiento de controles, buscar maneras de operar eficientemente, optimizar los recursos y velar por el cumplimiento de prácticas de sana administración pública.

RECOMENDACIONES

A la Junta de Retiro del Gobierno de Puerto Rico

1. Asegurarse que el administrador de la Junta de Retiro cumpla con las recomendaciones 2 y 3. **(Ver Hallazgos 1 al 9)**

Al administrador de la Junta de Retiro del Gobierno de Puerto Rico

2. Tomar las medidas necesarias para que:

    a. Se elabore y apruebe un Plan de Continuidad de Operaciones **(Ver Hallazgo 1.a).**

    b. Se actualicen el Análisis de Riesgo, el Plan de Recuperación de Desastres y el Plan de Manejo de Incidentes **(Ver Hallazgo 1.b)**.

c. Una vez aprobados, se revisen de forma periódica cada 24 meses, o cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica **(Ver Hallazgo 1.b).**

d. Se realice y se documente al menos un ejercicio y una prueba anualmente para todas sus unidades simulando escenarios de desastres o interrupción de negocios que garantice que su Plan de Continuidad de Negocio puede ser implementado en situaciones reales de emergencia y desastres **(Ver Hallazgo 1.c).**

e. Se designe una persona en la OTI, que no sea el director, responsable exclusivamente de la seguridad en los sistemas y por consiguiente de la ejecución de las funciones inherentes al plan de manejo de incidentes de sistemas de información **(Ver Hallazgo 3).**

f. Se asignen los recursos necesarios que colaboren con la actualización de las políticas, manuales operacionales, procedimientos, guías o documentación, para atemperarlos con las operaciones y circunstancias actuales. **(Ver Hallazgo 5).**

g. Se establezca un programa de capacitación para que se oriente al personal, entre otras cosas, sobre las políticas de seguridad, del uso adecuado de los sistemas de información y la importancia de salvaguardar las contraseñas. **(Ver Hallazgo 6).**

h. Impartir instrucciones a la directora del Área de Contraloría para que, junto al director interino de la OTI, realicen el análisis correspondiente y se establezcan las medidas necesarias de manera que, de ser necesario acceder y obtener cierta información, no se requiera la divulgación de las contraseñas. **(Ver Hallazgo 6).**

3. Impartir instrucciones al director interino de la OTI de que:

a. Se asegure que situaciones como las señaladas en el **Hallazgo 2.a** no se repitan.

b. Realice las gestiones necesarias para mantener al personal capacitado y actualizado en todo lo relacionado a las funciones o parámetros de seguridad de *Microsoft 365.* **(Ver Hallazgo 2.b).**

c. Se formule y apruebe un plan de manejo de incidentes de sistemas de información en el que se detallen los procesos de monitoreo, detección, investigación, respuesta y registro de incidentes de seguridad. **(Ver Hallazgo 3).**

d. Se prepare y mantenga actualizado el diagrama esquemático de la red. **(Ver Hallazgo 4).**

e. Se establezca un programa de adiestramientos periódicos para que el personal de la OTI obtenga los conocimientos actualizados y necesarios para realizar las funciones que les fueron asignadas. **(Ver Hallazgo 7.a y b).**

f. Coordine charlas periódicas para orientar al personal sobre las políticas y mejores prácticas de seguridad en el manejo de los recursos informáticos. **(Ver Hallazgo 7.c).**

g. Se elimine o desactive, si aún no lo ha hecho, la cuenta de acceso de la empleada que se separó del servicio. **(Ver Hallazgo 8)**.

h. Se realice una revisión periódica de las cuentas activas en los sistemas de información de la ASR. **(Ver Hallazgo 8)**.

i. Se implemente el requisito de códigos individuales para el uso de las multifuncionales. **(Ver Hallazgo 9).**

Al Principal Ejecutivo de Innovación e Información del Gobierno

4. Evaluar la implementación en las agencias de la licencia *Azure AD P2* de Microsoft (licencia E5). **(Ver Comentario Especial)**.

CONCLUSIÓN

La evaluación realizada a los documentos, y la información recopilada durante el examen, demostraron que las operaciones de la OTI en lo que concierne a los controles internos establecidos para la administración de la seguridad, el acceso lógico a los sistemas de información, procedimientos adecuados para el manejo de incidentes de seguridad, programa de continuidad del servicio y capacitación al personal, no se realizaron conforme a las normas y procedimientos generalmente aceptadas en este campo.

Con respecto a las operaciones realizadas por la Administración de los Sistemas de Retiro, en cuanto a la notificación inicial y de seguimiento mediante cartas circulares a las entidades gubernamentales sobre las cuentas correctas a utilizar para depositar el cargo *PayGo*, las aportaciones individuales, descuentos de préstamos y seguro por incapacidad, las mismas se efectuaron de conformidad a las normas aplicables. En cuanto a las medidas de mitigación tomadas una vez se detecta el incidente con los correos electrónicos fraudulentos enviados a las agencias, las gestiones a tiempo realizadas por el personal del Área de Contraloría y la División de Recaudaciones evitaron que el fraude se extendiera a otras entidades gubernamentales y que las autoridades de ley y orden pertinentes realizaran las acciones correspondientes.

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, 5 de octubre de 2021, en San Juan, Puerto Rico.

Ivelisse Torres Rivera
Inspectora General

INFORMACIÓN GENERAL

Misión

Consolidar los recursos y esfuerzos del Gobierno de Puerto Rico, para promover una sana administración pública y mediante una preintervención efectiva, el óptimo funcionamiento de sus instituciones.

Visión

Servir como entidad gubernamental reconocida a nivel local e internacional y lograr a través de auditorías internas y acciones preventivas, el funcionamiento efectivo y eficiente de los fondos y de la propiedad pública del Gobierno de Puerto Rico.

Línea de Consultas

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 de Consultas: 787-679-7979
- Correo Electrónico: informa@oig.pr.gov

Contactos


PO box 191733 San Juan, Puerto Rico 00919-1733


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


787-679-7997


consultas@oig.pr.gov


www.oig.pr.gov