INFORME DE AUDITORÍA TI-22-12

17 de junio de 2022

Sistema de Retiro para Maestros
del Estado Libre Asociado de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5350 - Auditoría 15526)

Período auditado: 26 de febrero al 30 de noviembre de 2021

CONTENIDO

Página

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

17 de junio de 2022

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos a la Oficina de Sistemas de Información (OSI) del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico (Sistema). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones de la OSI y de los sistemas de información del Sistema, se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

Evaluar el cumplimiento de la *Norma de Uso y Seguridad de los Recursos de Tecnología e Información* (*Norma de Uso y Seguridad*), aprobada el 12 de enero de 2012 por el entonces director ejecutivo interino del Sistema; y de las políticas incluidas en 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 entonces director de la Oficina de Gerencia y Presupuesto (OGP), entre otras, para determinar lo siguiente:

1. El Sistema cuenta con un análisis de riesgos, un plan de continuidad y un plan de contingencias completo y actualizado.

2. Los accesos otorgados a los usuarios del Sistema de Aportaciones y Beneficios Integrados (SABI) y de la aplicación PeopleSoft Finanzas (PeopleSoft) están documentados y autorizados; los privilegios de acceso se otorgan conforme a las funciones realizadas por estos usuarios; y las cuentas de acceso de exempleados, exconsultores y personal transferido son desactivadas.

CONTENIDO DEL INFORME

Este *Informe* contiene cinco hallazgos del resultado del examen que realizamos de los objetivos indicados. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 26 de febrero al 30 de noviembre de 2021. En algunos aspectos examinamos operaciones de fechas anteriores y posteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos, relacionados con los objetivos de auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la entidad auditada; y pruebas y análisis de procedimientos de control interno.

Al realizar esta auditoría, utilizamos la *Norma de Uso y Seguridad*; las *Normas de Resguardo y Recuperación de los Sistemas* (*Normas de Resguardo*), aprobadas el 14 de septiembre de 2011; y las políticas establecidas en la *Carta Circular 140-16*. Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica las guías establecidas en el *Federal Information System Controls*

Audit Manual (*FISCAM*)[1], emitido por el GAO. Aunque al Sistema no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgos.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Sistema se creó mediante la *Ley 91-2004*[2], *Ley del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico*, según enmendada. Esto, con el propósito principal de administrar el sistema de anualidades y pensiones de los maestros de Puerto Rico como una organización de servicios a los miembros de su matrícula. Con la *Ley 91-2004* se creó una nueva estructura organizacional con el fin de dotar al Sistema de agilidad y rapidez en los procesos que lleva a cabo; otorgarle autonomía gerencial y administrativa al separarlo de la intervención de otras agencias; establecer una política anticorrupción; y garantizar a los participantes el recibo de los beneficios que le corresponden en un tiempo justo. Además, mediante esta *Ley*, se transfirieron al Sistema todos los recursos y las funciones de la Junta de Retiro para Maestros, entre otros. También se transfirieron al Sistema todas las deudas, las obligaciones y las responsabilidades de dicha Junta.

La *Ley 91-2004* fue derogada por la *Ley 160-2013, Ley del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico*, que establecía la implementación de una reforma al sistema de retiro vigente hasta entonces. La *Ley 160-2013* fue impugnada por los grupos magisteriales y el Tribunal Supremo resolvió que no era de aplicabilidad a los participantes activos. Como resultado de esta decisión, el Sistema administra dos estructuras de beneficios: una de beneficios definidos, aplicable a todos los participantes nombrados en o antes del 1 de agosto de 2014 que no retiraron sus aportaciones; y otra de aportaciones definidas bajo lo dispuesto en la *Ley 160-2013*, aplicable a los participantes con aportaciones a partir del 1 de agosto de 2014.

[1] El *FISCAM* utiliza las guías emitidas por el National Institute of Standards and Technology.

[2] Derogó la *Ley Núm. 218 del 6 de mayo de 1951, Ley de Retiro para Maestros*.

Mediante la *Ley 106-2017*, *Ley para Garantizar el Pago a Nuestros Pensionados y Establecer un Nuevo Plan de Aportaciones Definidas para los Servidores Públicos*, se estableció, entre otras cosas, que el Sistema y la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura (ASR) serán dirigidos por la Junta de Retiro del Gobierno de Puerto Rico (Junta). Esto, en conformidad con la realidad fiscal y económica de Puerto Rico y a las disposiciones de la *Ley Pública 114-187, Puerto Rico Oversight, Management, and Economic Stability Act* (*PROMESA*).

La Junta está compuesta por los siguientes 13 miembros: el director ejecutivo de la Autoridad de Asesoría Financiera y Agencia Fiscal de Puerto Rico (AAFAF), quien además es su presidente; el secretario de Hacienda; el director de la OGP; el director de la Oficina de Administración y Transformación de los Recursos Humanos en el Gobierno de Puerto Rico; un representante de los maestros del Departamento de Educación; un representante de las corporaciones públicas; un representante de la Rama Judicial[3]; el presidente de la Federación de Alcaldes; el presidente de la Asociación de Alcaldes de Puerto Rico; y cuatro representantes del interés público[4].

La Junta debe nombrar a su director ejecutivo, quien tiene a su cargo la administración de los asuntos internos de la Junta; la dirección y coordinación de los trabajos; y la firma de los contratos que sean aprobados por el Comité de Contratación y la Junta. Además, la Junta es la encargada de designar al director ejecutivo del Sistema, quien ejerce las funciones de administrador para dirigir y supervisar las actividades técnicas y administrativas.

El Sistema está compuesto por la Oficina Ejecutiva, las áreas de apoyo y las operacionales. El Área de Apoyo está compuesta por las oficinas de Asuntos Legales, Recursos Humanos y Relaciones Laborales, Servicios Generales,

[3] Designado por el Pleno del Tribunal Supremo.

[4] Un maestro pensionado del Sistema de Retiro para Maestros, un pensionado del Sistema de Retiro de los Empleados del Gobierno de Puerto Rico, un representante de los miembros de la Policía de Puerto Rico nombrado por el gobernador y uno de libre selección por parte del gobernador.

Sistemas de Información y el Área Fiscal. El Área Operacional está compuesta por las áreas de servicios de Retiro y Préstamo. Cada una de estas áreas y oficinas es dirigida por un director, quien le responde al director ejecutivo del Sistema.

La estructura organizacional de la OSI está compuesta por la Oficina del Director y las siguientes cinco secciones: Desarrollo de Sistemas de Información, Base de Datos, Seguridad, Operaciones y Redes. Desde el 1 de agosto de 2021, la dirección de la OSI está a cargo del director de tecnología de información interino de la Junta. La OSI es la encargada de administrar los sistemas de información computadorizados del Sistema, y cuenta con un centro de cómputos localizado en la oficina principal del Sistema en San Juan.

Al 1 de noviembre de 2021, el Sistema contaba con 469 computadoras, 126 monitores, 40 *scanners*, 23 *switches*[5], 19 servidores, 17 impresoras y 3 *routers*[6], entre otros. Además, contaba con 28 sistemas y aplicaciones que se utilizaban para realizar y mantener sus operaciones. Entre estos se encontraban el SABI, utilizado para administrar las transacciones de los participantes que cotizan en el Sistema; y PeopleSoft, utilizada para administrar todas las transacciones de desembolsos.

Los recursos para financiar las actividades operacionales del Sistema provienen principalmente de las aportaciones patronales e individuales, los intereses sobre préstamos y las asignaciones provenientes del Fondo General del Gobierno del Estado Libre Asociado de Puerto Rico para cubrir beneficios garantizados a los pensionados mediante leyes especiales. El presupuesto aprobado para el Sistema, para los años fiscales del 2018-19 al 2020-21[7], ascendió a $21,977,296, $18,220,679 y $14,308,064, respectivamente.

---

[5] Dispositivo de comunicación central que conecta dos o más segmentos de red y que permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para lograr una comunicación más eficiente.

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

[7] Desde el año fiscal 2021-22, se consolidó en la Junta el presupuesto del Sistema y de la ASR.

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

El Sistema cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.srm.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Mediante correo electrónico del 5 de abril de 2022, remitimos el borrador de este *Informe*, para comentarios del Lcdo. Luis M. Collazo Rodríguez, director ejecutivo del Sistema.

El 5 de mayo de 2022 el director ejecutivo contestó y nos indicó, entre otras cosas, lo siguiente:

> […] Se utiliza como Criterio varias políticas y se hace referencia al cumplimiento con las mismas, pero la Carta Circular 2021-007, dejó sin efecto cualquier Carta Circular, Memorando, Orden Administrativa, Políticas, en particular las Políticas Núm. ATI 003 Seguridad de los Sistemas de Información y ATI 014, Manejo de Firewalls, Normativas, comunicación escrita o instrucción anterior de PRITS o publicada por la OGP como su predecesora antes de la aprobación de la Ley-75, que en todo o parte sea incompatible con esta, hasta donde existiera tal incompatibilidad. [*sic*]
>
> […] la Política Núm. ATI-015 fue promulgada al amparo de la Ley Núm. 151 de 22 de junio de 2004, según enmendada, vigente al momento de la aprobación de esta. Conforme a la Política, la OGP era la agencia encargada de velar por el cumplimiento con esta disposición en todas las agencias de la Rama Ejecutiva. Entendemos que esta política no le era extensible al Sistema de retiro para Maestros, pues en el Artículo 2.1 de la Ley Núm. 160-213, establece que "El Sistema es un organismo del Gobierno, independiente y separado de otros". Es decir, no es un organismo adscrito a la Rama Ejecutiva a quien le aplicara la referida política. [*sic*]
>
> […] se utiliza como Criterio el FISCAM, que es una guía que pretende proporcionar orientación para realizar, de manera eficaz y eficiente, controles y auditorías en los Sistemas de Información […] [*sic*]

Evaluamos los comentarios del director ejecutivo, con respecto a los criterios utilizados en los hallazgos del borrador de este *Informe*, y determinamos que, a la fecha de la auditoría, al Sistema le aplicaban las

políticas de la *Carta Circular 140-16*, incluida la *Política ATI-003*. Esto según se indica en la sección Aplicabilidad de dicha *Carta Circular*. Además, mediante la *Ley 106-2017* se estableció que el Sistema será dirigido por la Junta la cual es parte de la Rama Ejecutiva.

Por otro lado, la *Carta Circular 2021-007, Establecimiento de la Política Cibernética*, fue emitida el 6 de diciembre de 2021 por el director ejecutivo del Puerto Rico Innovation and Technology Service (PRITS) y, a esta fecha, ya había terminado el período de la auditoría. En la **Recomendación 2** se hace referencia al cumplimiento de esta *Carta Circular* para propósitos de implementar las acciones correctivas correspondientes. Además, según establecido en la sección **ALCANCE Y METODOLOGÍA**, aunque utilizamos las guías del *FISCAM* en algunos de los hallazgos, al Sistema no se le requiere cumplir con estas. Sin embargo, entendemos que, para las situaciones señaladas en las que el Sistema no cuenta con reglamentación interna, estas guías representan las mejores prácticas en el campo de la tecnología de información.

Otros comentarios remitidos por el director ejecutivo se consideraron en la redacción final de este *Informe* y algunos se incluyeron en los **hallazgos**.

CONTROL INTERNO

La gerencia del Sistema es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de lo siguiente:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de esta auditoría. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno del Sistema.

En los **hallazgos** se comentan las deficiencias de controles internos significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión Cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI del Sistema, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 5**, que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con el informe de análisis de riesgos de los sistemas de información computadorizados

Situación

a. Un análisis de riesgos es un proceso mediante el cual se identifican los activos de sistemas de información, sus vulnerabilidades y las amenazas a las que se encuentran expuestos. Además, se establecen medidas y controles para evitar o disminuir los riesgos y proteger los activos. Toda entidad gubernamental debe realizar un análisis de riesgos, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

   El Sistema cuenta con el *Entregable 2: Documento de Estimación y Análisis de Riesgo* (*Análisis de Riesgo*). Este fue preparado y entregado por una compañía externa y aceptado por el Sistema el 19 de mayo de 2009.

El examen realizado el 16 de noviembre de 2021 reveló que este análisis carecía de lo siguiente:

1) Un inventario de activos de los sistemas de información que detallara los equipos, programas y datos del Sistema. Esto, con su valoración y 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.

2) La identificación de las posibles amenazas contra los sistemas de información y la probabilidad de que ocurran las mismas.

Criterios

La situación comentada se aparta de lo establecido en la Sección A. de la *Política ATI-003, Seguridad de los Sistemas de Información*, y en la Sección C. de la *Política ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Efecto

La situación comentada impide al Sistema estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas principales de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información.

Causa

Lo comentado se atribuye a que en el Sistema no habían considerado incluir como parte del análisis de riesgos, los aspectos mencionados en la situación.

Comentarios de la Gerencia

El director ejecutivo nos indicó, entre otras cosas, lo siguiente:

> […] existe un inventario de los activos de los Sistemas de Retiro para Maestros que cumple con los elementos que se desglosan en el informe. Se contaba con el inventario al momento de finalizar el informe, pero los auditores no corroboraron con la Oficina de Sistemas de Información de los Sistemas de Retiro para Maestros antes de emitir el informe. [*sic*]

Consideramos las alegaciones del director ejecutivo, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que el *Análisis de Riesgo* evaluado no incluía el inventario de activos de los sistemas. Durante la auditoría nos suministraron el inventario de propiedad. Sin embargo, este no era parte del *Análisis de Riesgo* y no incluía todos los aspectos indicados en el **Hallazgo**. Además, en la contestación al borrador de este *Informe* no remitieron evidencia del inventario al que hacen referencia.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de actualización de información en la Estrategia de Tecnología y en otros documentos entregables del Sistema

Situación

a. Las entidades gubernamentales deben desarrollar un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones basado en un análisis de riesgos. Estos planes deben establecer, entre otras cosas, las estrategias de respuesta, recuperación, reanudación y restauración para todos los procesos principales de la entidad. Estos planes deben ser actualizados cada vez que se incorpore un sistema o aplicación crítica en la entidad o cuando se realice un cambio significativo dentro de su infraestructura operacional.

   Además, toda entidad gubernamental debe contar con un plan de contingencias para restablecer sus operaciones más importantes 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 los sistemas de información computadorizados.

   El Sistema contaba con el *Entregable 4: Documento Estrategia de Tecnología* (*Estrategia de Tecnología*) del 28 de junio de 2009, que incluía las actividades concernientes para prevenir y asegurar que la plataforma tecnológica que apoyaba los procesos críticos del negocio fuera reanudada después de un desastre. Esto, para que pudiera continuar su operación y satisfacer las necesidades de sus clientes externos e internos. También se enfocaba en los procesos de negocios

y establecía los procedimientos y sistemas necesarios para asegurar la continuación de los servicios indispensables. Además, el Sistema contaba con otros 11 documentos entregables que estaban relacionados con el plan de recuperación de desastres. El propósito de estos era proveer una guía documentada que permitiera recuperar, restaurar y mantener en operación las funciones tecnológicas y de negocio más críticas cuando ocurriera un incidente que potencialmente pudiera afectar al Sistema y generar una interrupción en el Centro de Datos.

El examen realizado el 9 de noviembre de 2021 a la *Estrategia de Tecnología* y a los otros documentos entregables reveló que la información contenida en estos no estaba actualizada, según se indica:

1) Las aplicaciones implementadas luego del 28 de junio de 2009 no estaban incluidas.

2) Como parte de la infraestructura para la continuidad de las operaciones incluían sucursales[8] que fueron cerradas.

3) Como parte de los procesos de recuperación incluían la definición de un centro alterno que no existe.

4) Incluían nombres de servidores, sistemas operativos, bases de datos y versiones de aplicaciones que no existían a la fecha del examen.

5) Los nombres incluidos del personal perteneciente al equipo funcional ya no laboraban en el Sistema.

Criterios

La situación comentada es contraria a lo establecido en la Sección B.1 de la *Política ATI-003* y en las secciones D y E de la *Política ATI-015* de la *Carta Circular 140-16*. Además, se aparta de lo establecido en el Capítulo 3.5, Contingency Planning, del *FISCAM*.

[8] Sucursales o centros de orientación y servicios a participantes y pensionados que estaban localizados en Arecibo, Caguas, Humacao, Mayagüez y Ponce. Estos brindaban servicios de orientación a participantes y pensionados.

Efecto

La situación comentada puede propiciar la improvisación y que, en casos de emergencia, se tomen las medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios ofrecidos a los usuarios de los sistemas de información computadorizados del Sistema.

Causa

Lo comentado se atribuye a que el director de la OSI no había realizado las gestiones necesarias para actualizar la *Estrategia de Tecnología* y los otros documentos entregables.

Véanse las recomendaciones 1 y 3.a.

Hallazgo 3 - Falta de almacenamiento de los respaldos fuera de los predios del Sistema y de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Las entidades deben establecer procedimientos para respaldar periódicamente la información y los programas computadorizados, y almacenarlos en un lugar seguro y distante de sus predios. Esto, para que, de ocurrir una emergencia o desastre que afecte las instalaciones principales de la entidad, los respaldos estén disponibles para poder recuperar la mayor cantidad de información.

   Al 4 de mayo de 2021, en el Sistema se realizaban respaldos de forma automática en la librería de discos virtuales[9] localizada en el Centro de Datos[10]. Los respaldos diarios eran realizados de forma automática durante las noches. Estos se realizaban a las bases de datos[11], los repositorios de documentos de los empleados (Fólder Z), la información que los usuarios mantienen en *Desktop* y en *My Documents*, las aplicaciones desarrolladas internamente y a las

[9] *Virtual Tape Library* (*VTL*), por sus siglas en inglés.

[10] Área ubicada en la OSI donde estaban los servidores.

[11] De las aplicaciones *People Soft*, Originación y Mantenimiento de Préstamos (OMP) y la aplicación interna de Recursos Humanos, la cual se utiliza para llevar la asistencia de los empleados del Sistema.

configuraciones e información del *Active Directory*. En la mañana siguiente, los respaldos de la base de datos eran comprimidos y el especialista en microcomputadoras y redes de comunicación o el administrador de la base de datos los movían manualmente de la base de datos de la librería de discos virtuales a la nube que utiliza el Sistema.

Nuestro examen reveló que, al 4 de mayo de 2021, las copias de los respaldos que incluían los repositorios de documentos de los empleados, de la información que los usuarios mantenían en el *Desktop* y en *My Documents*, de las aplicaciones desarrolladas internamente y de las configuraciones e información del *Active Directory*, no se mantenían en un lugar seguro fuera de los predios del Sistema.

b. Como parte integral del plan de continuidad de negocios de una entidad, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios.

   Al 11 de mayo de 2021, el Sistema no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

Criterios

La situación comentada en el **apartado a.** se aparta de lo establecido en la sección g. de las *Normas de Resguardo*. Además, las situaciones comentadas se apartan de lo establecido en el Capítulo 3.5 del *FISCAM*.

Efectos

La situación comentada en el **apartado a.** puede ocasionar que, en casos de emergencias, el Sistema no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Lo comentado en el **apartado b.** podría afectar las operaciones del Sistema, y los servicios de los sistemas de información computadorizados, ya que no tendrían disponibles unas instalaciones externas para operar después de una

emergencia o un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de los archivos y el pronto restablecimiento de las operaciones normales del Sistema.

Causas

El entonces director interino de la OSI atribuyó la situación comentada en el **apartado a.** a que dicha Oficina no tiene presupuesto asignado para transportar o exportar los respaldos a un lugar externo fuera de los predios del Sistema.

Además, atribuyó lo comentado en el **apartado b.** a que el centro alterno se encontraba en la Sucursal de Ponce, pero la misma cerró sus operaciones.

Comentarios de la Gerencia

El director ejecutivo nos indicó, entre otras cosas, lo siguiente:

> […] Tenemos reparos en cuanto al planteamiento sobre que no tenemos el centro alterno para restaurar sus operaciones criticas computadorizadas en casos de emergencias. Aunque no se tenía para la fecha mencionada, antes de concluir el periodo que comprende la auditoría, ya se contaba contratado el servicio de almacenamiento en la nube con la compañía Microsoft Azure [*sic*]

Consideramos las alegaciones del director ejecutivo, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que, según la información suministrada durante la auditoría, el servicio contratado al que se hace referencia es utilizado solamente para el almacenamiento de los respaldos de información de las bases de datos. **[Apartado a.]** Además, este servicio es de almacenamiento y no representa un centro alterno para la restauración de las operaciones críticas computadorizadas. **[Apartado b.]**

Véanse las recomendaciones 1, 3.b. y c., y 4.a.

Hallazgo 4 - Deficiencias relacionadas con la administración y documentación de cuentas de acceso activas en el SABI y PeopleSoft

Situaciones

a. La información y los programas de aplicación utilizados en las operaciones de las entidades gubernamentales deben tener controles de acceso para su utilización, de manera que solamente el personal

autorizado pueda ver los datos necesarios o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deben incluir mecanismos de autenticación y autorización.

En la *Norma de Uso y Seguridad* se establece que la asignación, la modificación y la cancelación de acceso a los recursos de la red y las aplicaciones del Sistema deben ser enviadas a la OSI mediante el Portal de Asistencia a Usuarios[12]. Cada supervisor de área es responsable de solicitar al dueño de la aplicación (administrador o encargado de la aplicación en su área) o al director, la asignación, modificación y cancelación de accesos y privilegios para los recursos que estén bajo su supervisión. Además, se establece que cada dueño de aplicación y director de área, encargados de sistemas aplicativos, son responsables de la revisión de accesos, al menos, cada seis meses o períodos más cortos si así lo estiman necesario. Si el dueño de una aplicación o director de área no tiene la capacidad de ver los accesos directamente en la aplicación, debe pedir a la OSI los informes de accesos de usuarios para poder revisar los mismos.

La función de crear, modificar y desactivar las cuentas de acceso de las aplicaciones del Sistema era realizada por el oficial de seguridad de sistemas de informática. Los supervisores de las oficinas del Sistema eran responsables de solicitar, mediante el Sistema de Ticket o correo electrónico, los accesos del personal que supervisaban.

En el 2010, se adquirió el SABI para administrar las transacciones de los participantes que cotizan en el Sistema. Al 31 de mayo de 2021, el SABI contaba con 170 cuentas de acceso asignadas a 158 usuarios activos, quienes realizaban transacciones de acuerdo con los permisos de acceso asignados.

[12] En el Sistema también se conocía como Portal de Ticket. Actualmente cuentan con el Sistema de Ticket.

Los permisos existentes en el SABI eran Administrador, Administrador de Sistema, Director, Supervisor, Técnico, Operador, y Consulta.

1) El examen realizado el 15 de septiembre de 2021 sobre la documentación relacionada con la solicitud y autorización de una muestra de 11 usuarios activos en el SABI, al 31 de mayo de 2021, que tenían más de una cuenta de acceso asignada, reveló lo siguiente:

    a) No se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para solicitar y autorizar la creación de nueve cuentas de acceso asignadas a seis usuarios.

    b) La documentación entregada para solicitar y autorizar la creación de las cuentas de acceso no incluía lo siguiente:

        (1) La solicitud y autorización para la creación de cinco cuentas de acceso asignadas a tres usuarios

        (2) El nombre de las cuatro cuentas a las que se autorizaba el acceso asignadas a dos usuarios

        (3) La unidad de trabajo a la que tenían acceso para seis cuentas de acceso asignadas a cuatro usuarios

        (4) El tipo de permiso[13] autorizado para cinco cuentas de acceso asignadas a tres usuarios

        (5) La justificación para la creación de ocho cuentas de acceso asignadas a cinco usuarios.

2) El examen realizado el 15 de octubre de 2021 sobre la documentación relacionada con la solicitud y autorización de accesos otorgados a una muestra de 11 usuarios activos en el

[13] Se refiere al privilegio de acceso otorgado a las cuentas.

SABI, al 31 de mayo de 2021, con cuentas de acceso que tenían más de un permiso asignado, reveló que de 113 permisos otorgados:

a) No se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para la solicitud y autorización de 96 permisos otorgados a las cuentas de acceso asignadas a 10 usuarios.

b) De la documentación entregada para solicitar y autorizar los restantes 17 permisos otorgados a las cuentas de acceso asignadas a 5 usuarios, determinamos lo siguiente:

(1) No se incluyó la justificación para la asignación de 16 permisos otorgados a 5 cuentas de acceso.

(2) Ocho permisos, otorgados a dos cuentas de acceso, no correspondían a los que fueron autorizados.

(3) Dos permisos (técnico y director), otorgados a una cuenta de acceso, no incluían autorización.

3) El examen realizado el 30 de noviembre de 2021 sobre los permisos otorgados a una muestra de 12 usuarios activos en el SABI, al 31 de mayo de 2021, para determinar si el acceso otorgado fue basado en las funciones asignadas y a su puesto, reveló lo siguiente:

a) Existían cuatro cuentas de acceso asignadas a tres usuarios con permisos que no correspondían a las funciones de sus puestos, según se indica:

(1) La oficial de servicios de retiro auxiliar tenía asignada una cuenta con permiso de administrador de sistemas, que solo debe otorgarse a las cuentas de los empleados de la OSI.

(2) El oficial de seguridad de sistemas de informática tenía asignada una cuenta de acceso que, además del permiso de administrador de sistema correspondiente a su puesto,

tenía el permiso de supervisor. Este permiso es otorgado a empleados que tienen asignadas funciones de supervisión en el Área de Servicios de Retiro, o de mayor jerarquía.

(3) Una voluntaria del Programa de Voluntariado[14] tenía asignada dos cuentas de acceso con el permiso de técnico. Este permite realizar transacciones relacionadas con los casos de participantes, tales como añadir, modificar o eliminar data demográfica o numérica. Este permiso es otorgado a empleados que tienen asignadas funciones técnicas o de mayor jerarquía.

b) Cuatro cuentas de acceso con permisos de técnico asignadas a una exempleada y a una exvoluntaria, que cesaron sus funciones entre el 28 de febrero de 2020 y el 20 de noviembre de 2020, no se habían desactivado. Esto, luego de haber transcurrido entre 388 y 654 días desde la fecha de separación de estas y el 13 de diciembre de 2021[15].

b. En el 2006 se adquirió PeopleSoft para administrar todas las transacciones de desembolsos que se generan en el Sistema. Al 31 de mayo de 2021, esta aplicación contaba con 102 cuentas de acceso activas.

Del examen realizado el 21 de octubre de 2021 sobre la documentación relacionada con la solicitud y autorización de una muestra de 16 cuentas de acceso asignadas a 14 usuarios activos en PeopleSoft, determinamos que no se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para la solicitud y autorización de 10 cuentas de acceso asignadas a 9 usuarios.

---

[14] En la *Orden Administrativa Núm. 2011-05*, se estableció el registro de voluntariados, a tenor con la *Ley 261-2004, Ley de Voluntariado de Puerto Rico*, según enmendada.

[15] A esta fecha, observamos imágenes de pantalla del *Registro de Usuario* del SABI que indicaban que estas cuentas se encontraban activas.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la Sección 14 de la *Norma de Uso y Seguridad*, y en la Sección E.3 de la *Política ATI-003* de la *Carta Circular 140-16*. Lo comentado en el **apartado a.3)b)** también se aparta de lo establecido en la Sección 16 de la mencionada norma.

Efectos

Las situaciones comentadas le impiden al Sistema mantener un control efectivo y eficaz sobre las cuentas de acceso y los permisos asignados a estas. Además, propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta. También propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichas aplicaciones, sin que se puedan detectar a tiempo para fijar responsabilidades.

Causas

El oficial de seguridad de sistemas de informática atribuyó las situaciones comentadas en los **apartados a.1)a) y 2)a), y b.** a que la información relacionada con la solicitud y autorización para la creación de las cuentas de acceso del SABI pudo ser extraviada por problemas con el servidor del Portal de Ticket o problemas en el envío al correo electrónico por parte del solicitante. Además, atribuyó la situación comentada en el **apartado a.3)b)** a que los supervisores o directores del Área de Servicios de Retiro y Finanzas no realizan una revisión detallada de la lista de empleados que tienen cuentas activas, que él les envía mensualmente, para que la verifiquen y le notifiquen los empleados que ya no trabajan en el Sistema. Esto, para desactivar las cuentas de acceso asignadas a los exempleados del Sistema.

El director del Área de Servicios de Retiro atribuyó las situaciones comentadas en el **apartado a.1)b) y 2)b)** a que el Sistema no cuenta con un método uniforme automatizado que requiera que se registre información necesaria para la creación de las cuentas de acceso en el SABI y, al tramitarlo por *ticket* o correo electrónico, se pudiese obviar información que es importante para la creación de las cuentas. Además, atribuyó la situación

comentada en el **apartado a.3)a)** a que el Sistema no cuenta con el personal suficiente, en comparación con el volumen de casos que trabajan, para llevar a cabo las tareas que son requeridas en el Área de Servicios de Retiro.

Véanse las recomendaciones 1, 3.d., 4.b. y 5.

Hallazgo 5 - Falta de actualización de los sistemas operativos de los servidores donde residen las principales aplicaciones del Sistema

Situación

a. El sistema operativo controla la ejecución de los programas de computadoras y provee servicios, tales como asignación de recursos, planificación, controles de entrada y salida, y administración de datos. Las entidades deben verificar y actualizar periódicamente los sistemas operativos de los servidores para protegerlos de vulnerabilidades conocidas, y asegurarse de que los mismos funcionen adecuadamente.

   Nuestro examen reveló que, al 21 de abril de 2021, los sistemas operativos de los servidores donde residen el SABI, PeopleSoft y sus bases de datos no estaban actualizados. En dicha fecha, el especialista en microcomputadoras y red de comunicaciones nos informó que los servidores, donde reside el SABI y su base de datos, tienen instalado el sistema operativo Windows Server 2008. Además, nos indicó que los servidores, donde reside PeopleSoft y su base de datos, tienen instalados los sistemas operativos Windows Server 2003 y Windows Server 2008, respectivamente. Estos sistemas operativos no cuentan con el apoyo técnico del proveedor desde el 14 de julio de 2015 y 14 de enero de 2020.

Criterio

La situación comentada es contraria a lo sugerido en el Capítulo 3.3, Configuration Management, del *FISCAM*.

Efectos

La situación comentada aumenta los riesgos de ataques maliciosos a los servidores a través de las vulnerabilidades del sistema operativo, lo que podría ocasionar la pérdida de información personal de los clientes del

Sistema. Además, priva al Sistema de los servicios de apoyo técnico necesarios para garantizar la continuidad de las operaciones de estos servidores.

Causas

El director de la OSI atribuyó la situación comentada a que el Sistema estaba en proceso de adquirir equipos más robustos y modernos que pudieran garantizar la operación de la agencia. En relación con los servidores donde reside el SABI, no han podido ser actualizados debido a que se debe revisar la matriz de compatibilidad de Oracle para realizar la migración de forma escalonada.

Además, los servidores donde reside la aplicación PeopleSoft no han podido ser actualizados, debido al grado de complejidad y el costo que requiere dicho proceso.

Véanse las recomendaciones 1 y 3.e.

RECOMENDACIONES

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

1. Asegurarse de que el director ejecutivo cumpla con las **recomendaciones de la 2 a la 4. [Hallazgos del 1 al 5]**

Al director ejecutivo del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico

2. Asegurarse de que se revise el *Análisis de Riesgo* del Sistema para que incluya un inventario de los activos de sistemas de información, la identificación de las posibles amenazas contra estos y la probabilidad de que ocurran las mismas. **[Hallazgo 1]** Una vez revisado, lo remita para su aprobación y vea que se actualice cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Sistema.

3. Asegurarse de que el director de la OSI cumpla con lo siguiente:

    a. Revise y actualice la información incluida en la *Estrategia de Tecnología* y en los otros entregables para que en estos se incluya la información relacionada con los aspectos comentados. Una vez revisados, los remita para su aprobación y vea que estos se

revisen cada vez que ocurra un cambio significativo dentro de la estructura operacional y tecnológica del Sistema. Esto, para asegurarse de que los mismos se mantengan actualizados. **[Hallazgo 2]**

b. Almacene una copia de los respaldos de la información que los usuarios mantienen en el *Desktop* y en *My Documents*, de las aplicaciones desarrolladas internamente y de las configuraciones e información del *Active Directory* en un lugar seguro. Este no debe estar expuesto a las mismas amenazas de desastre que el Centro de Datos del Sistema. **[Hallazgo 3-a.]**

c. Identifique un centro alterno que no esté expuesto a los mismos riesgos que el área de sistemas de información, y que cuente con la infraestructura y los equipos necesarios para restaurar las operaciones computadorizadas críticas del Sistema, en caso de emergencia. **[Hallazgo 3-b.]**

d. Imparta instrucciones al oficial de seguridad de sistemas de informática para lo siguiente:

1) Cumpla con las directrices establecidas en la *Norma de Uso y Seguridad* relacionadas con la solicitud y creación de las cuentas de acceso, y de la revisión periódica de accesos. **[Hallazgo 4-a.1) y 2), y b.]**

2) Mantenga un respaldo de las solicitudes y autorizaciones, tramitadas a través del Sistema de Ticket y de los correos electrónicos que documentan la creación de las cuentas de acceso. **[Hallazgo 4-a.1)a) y 2)a), y b.]**

3) Establezca un método uniforme que requiera el registro de información necesaria para la solicitud y autorización para la creación de las cuentas de acceso de los usuarios en el Sistema. **[Hallazgo 4-a.1)b) y 2)b)]**

4) Desactive las cuentas de acceso comentadas en el **Hallazgo 4-a.3)b)**, y vea que, en lo sucesivo, se desactiven en el momento en que el usuario cese sus funciones.

e. Actualice los sistemas operativos de los servidores donde residen el SABI y PeopleSoft, para así asegurar un funcionamiento efectivo y eficaz de los sistemas de información del Sistema. **[Hallazgo 5]**

4. Identificar alternativas costo-efectivas que permitan lo siguiente:

a. Mantener los respaldos de los repositorios de documentos de los empleados, la información que los usuarios mantienen en el *Desktop* y en *My Documents*, las aplicaciones desarrolladas y las configuraciones del *Active Directory*, en un lugar externo fuera de los predios del Sistema **[Hallazgo 3.a)]**

b. Asignar más personal para realizar las tareas requeridas en el Área de Servicios de Retiro. **[Hallazgo 4-a.3)a)]**

5. Asegurarse de que el director del Área de Servicios de Retiro cumpla con lo siguiente:

a. Documente la solicitud y autorización para la creación de las cuentas de acceso y de los permisos asignados a estas, según mencionado en el **Hallazgo 4-a.1) y 2), y b.** Además, de que cumpla con las directrices establecidas en la *Norma de Uso y Seguridad* relacionadas con la solicitud y creación de las cuentas de acceso, y la revisión periódica de accesos.

b. Revise los accesos y permisos asignados a los usuarios del SABI para que estén de acuerdo con las funciones y responsabilidades de los puestos de los usuarios. **[Hallazgo 4-a.3)a)]**

c. Imparta instrucciones para que los supervisores del Área de Servicios de Retiro revisen la lista enviada mensualmente por el oficial de seguridad de sistemas de informática, con los empleados con cuentas de acceso activas en las aplicaciones del Sistema. Esto, para que le notifiquen al oficial de seguridad de sistemas de

informática aquellas cuentas de acceso asignadas a usuarios que no laboran en el Sistema, para que las mismas sean desactivadas. **[Hallazgo 4-a.3)b)]**

APROBACIÓN

A los funcionarios y a los empleados del Sistema, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por: 

ANEJO 1

SISTEMA DE RETIRO PARA MAESTROS
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

MIEMBROS PRINCIPALES DE LA JUNTA DE RETIRO DEL GOBIERNO DE PUERTO RICO DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO[16]	PERÍODO	
		DESDE	HASTA
Lcdo. Manuel González Del Toro	Presidente	30 oct. 21	30 nov. 21
Lcdo. Carlos Saavedra Gutiérrez	"	1 mar. 21	29 oct. 21

[16] Designados como presidentes de la Junta por el director ejecutivo de la AAFAF, en su representación.

ANEJO 2

SISTEMA DE RETIRO PARA MAESTROS
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Luis M. Collazo Rodríguez	Director Ejecutivo	26 feb. 21	30 nov. 21
Sr. Fernando Marte Soto	Subdirector Ejecutivo	26 feb. 21	30 nov. 21
Sra. Irma Y. Suárez Sánchez	Directora de Recursos Humanos y Relaciones Laborales	26 feb. 21	30 nov. 21
Sr. Reynaldo Agosto Loubriel	Director Área Servicios de Retiro	26 feb. 21	30 nov. 21
Dr. Víctor Robles Ramírez[17]	Director de la Oficina de Sistemas de Información	1 ago. 21	30 nov. 21
Dr. Ibrahim López Rivera	Director Oficina Sistemas de Información (Interino)	26 feb. 21	31 jul. 21

[17] Efectivo el 1 de agosto de 2021, fue designado a realizar las funciones de director de la Oficina de Sistemas de Información. Sin embargo, su puesto oficial es director de tecnología de información interino de la Junta.

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr