INFORME DE AUDITORÍA TI-20-10

4 de junio de 2020

Autoridad de Tierras de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5180 - Auditoría 14377)

Período auditado: 8 de abril al 27 de agosto de 2019

CONTENIDO

Página

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

4 de junio de 2020

A la Gobernadora, 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) de la Autoridad de Tierras de Puerto Rico (Autoridad). 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 de la Autoridad se efectuaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

Determinar si las operaciones de la OSI; en lo que concierne a los controles para la administración de la seguridad, el acceso lógico y la continuidad del servicio; se efectuaron, en todos los aspectos significativos, de acuerdo con la reglamentación interna de la Autoridad y 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, entre otras; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este *Informe* contiene seis hallazgos sobre el 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 8 de abril al 27 de agosto de 2019. En algunos aspectos examinamos transacciones de fechas anteriores. 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 Estados Unidos (GAO, por sus siglas en inglés), en lo que 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 la 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 unidad auditada; y pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

Al realizar esta auditoría utilizamos como criterios lo siguiente:

- *Reglamentación y Procedimiento para los Sistemas de Información*, aprobado el 26 de abril de 2007 por el entonces director ejecutivo y la Junta de Gobierno (Junta)
- *Normas y Procedimientos para la Instalación y Configuración de la Red*, aprobado el 4 de junio de 2012 por el entonces director ejecutivo
- *Normas y Procedimientos del Departamento de Sistemas de Información*, aprobado el 4 de junio de 2012 por el entonces director ejecutivo
- *Plan para el Manejo y Seguridad de los Resguardos (Backup)*, aprobado el 4 de junio de 2012 por el entonces director ejecutivo

- Las políticas incluidas 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 Systems Controls Audit Manual* (FISCAM)[1], emitido por el GAO. Aunque a la Autoridad 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

La Autoridad fue creada por la *Ley Núm. 26 del 12 de abril de 1941, Ley de Tierras de Puerto Rico*, según enmendada, para implementar la política agraria de Puerto Rico, y para eliminar la gran concentración de tierras en manos corporativas. Además, para asegurar a los individuos la conservación de sus tierras, ayudar a la formación de nuevos agricultores y facilitar el aprovechamiento de las tierras para el mayor bien público. Conforme al *Plan de Reorganización 4 del 29 de julio de 2010*, conocido como el *Plan de Reorganización del Departamento de Agricultura de 2010*, la Autoridad pasó a ser un componente programático y operacional del Departamento de Agricultura (Departamento). La Autoridad tiene como misión adquirir, custodiar y administrar los terrenos de más alto valor productivo con el propósito de fomentar la agricultura autosostenible y rentable, potenciar el desarrollo socioeconómico de la sociedad puertorriqueña y garantizar la permanencia de los mejores terrenos de labranza a las futuras generaciones.

Los poderes y las políticas generales de la Autoridad son determinados por una Junta, compuesta por el secretario de Agricultura (secretario), quien es su presidente, y seis miembros adicionales que nombra el gobernador de Puerto Rico. Estos desempeñan sus funciones según establece la autoridad nominadora y hasta que sus sucesores sean

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

nombrados y tomen posesión de sus cargos. De los seis miembros, tres son nombramientos *ex officio*: el secretario de Desarrollo Económico y Comercio, el director ejecutivo de la Autoridad de Asesoría Financiera y Agencia Fiscal de Puerto Rico y el presidente del Banco de Desarrollo Económico para Puerto Rico, o sus respectivos representantes autorizados. Estos son específicamente designados por notificación previa al secretario, y deben ser funcionarios que respondan directamente a quien representan y se hagan responsables de las decisiones y determinaciones que se tomen en la Junta. Los tres miembros restantes son nombrados en representación del sector agrícola y agro-industrial de Puerto Rico por un término de cuatro años.

Los reglamentos de la Autoridad y los de cada una de las subsidiarias, los cuales son aprobados por la Junta, podrán disponer que se deleguen en los directores ejecutivos o en otros funcionarios, agentes o empleados, aquellos poderes y deberes de la Autoridad y de las subsidiaras que la Junta estime propios.

La Autoridad cuenta con un director ejecutivo nombrado por la Junta, con la aprobación del gobernador de Puerto Rico. La Autoridad cuenta con una corporación subsidiaria[2] que es dirigida por un director ejecutivo. Este es nombrado por el director ejecutivo de la Autoridad, con la aprobación de la Junta. Cada director ejecutivo es el primer funcionario ejecutivo de su respectiva organización, desempeña los deberes y tiene las responsabilidades y autoridades que sean prescritas por la autoridad nominadora.

La estructura organizacional de la Autoridad consiste de las oficinas de Director Ejecutivo, Director Ejecutivo Auxiliar, Auditoría Interna, Servicios Generales, y Sistemas de Información; los departamentos de Recursos Humanos y Relaciones Laborales, Finanzas, Contabilidad y Presupuesto, Legal, Bienes Raíces, y Operaciones de Campo; y el Programa de Fincas Familiares.

[2] El Fondo de Innovación para el Desarrollo Agrícola de Puerto Rico (FIDA) es una subsidiaria de la Autoridad creada mediante la *Resolución Corporativa* de la Junta de la Autoridad del 30 de octubre de 2001 y aprobada por el entonces gobernador interino de Puerto Rico el 9 de enero de 2002.

La OSI le responde al director ejecutivo auxiliar de la Autoridad y cuenta con seis puestos autorizados, de los cuales tres están ocupados: oficial principal de informática, técnico en sistemas de información y administradora en sistemas de oficina III. Los puestos vacantes son: gerente de sistemas de información, coordinador de servicios de sistemas de información, y administrador de bases de datos.

A la fecha de nuestra auditoría, la Autoridad tenía una red local de área (LAN, por sus siglas en inglés) que interconectaba, aproximadamente, a 75 usuarios, mediante tecnología de fibra óptica, cables y conexión inalámbrica. Además, utilizaba firewall[3] y servicios proxy[4]. La red de la Autoridad tenía en operación 6 servidores físicos y 15 virtuales, 11 *switches*[5], 3 *routers*[6] y 84 computadoras. El acceso a Internet lo proveía una compañía externa. Además, mantenían en producción cuatro aplicaciones adquiridas: HR Sense, para el manejo de Recursos Humanos; Trutime, para el manejo de asistencia; Oracle, para manejar las operaciones y transacciones financieras de la Autoridad; y ARCGIS, para ver mapas de las fincas de la Autoridad y para manejar los inventarios de los terrenos e identificar las fincas, su tamaño y uso, y el cliente arrendado.

Los recursos para financiar las operaciones de la Autoridad provienen de ingresos propios. El presupuesto aprobado para los años fiscales del 2016-17 al 2018-19, ascendió a $9,437,000, $7,551,000, y $9,681,000, respectivamente. Durante los años fiscales del 2016-17 al 2018-19, la Autoridad asignó a la OSI un presupuesto de $384,118, $216,914, y $150,270, respectivamente.

---

[3] Un *firewall* o cortafuegos es un programa informático o un *hardware* que brinda protección a una computadora (ordenador) o a una red frente a intrusos.

[4] Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.

[5] Dispositivo que permite la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

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

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

La Autoridad cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.agricultura.pr/autoridad-tierras. Esta página provee información acerca de la Autoridad y de los servicios que presta.

COMUNICACIÓN CON LA GERENCIA

El borrador de este *Informe* se remitió al Agro. Juan L. Rodríguez Reyes, director ejecutivo, para comentarios, mediante correo electrónico del 7 de abril de 2020.

El director ejecutivo contestó mediante carta del 4 de mayo de 2020. En los hallazgos que contestó, se incluyeron sus comentarios.

CONTROL INTERNO

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

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

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para 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 de la Autoridad.

En los **hallazgos del 1 al 5** se comentan deficiencias de control interno significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado. Además, en el **Hallazgo 6** se comenta una deficiencia de control interno relacionada con los controles

ambientales y físicos en las áreas de servidores y distribución de cableado, la cual no es significativa para los objetivos de esta auditoría, pero merece que se tomen acciones correctivas.

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 de la Autoridad objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

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

Situación

a. El análisis de riesgos es un proceso mediante el cual se identifican los activos de los sistemas de información, sus vulnerabilidades y las amenazas a las que están expuestos. Además, se establecen medidas de seguridad y controles adecuados para evitar o disminuir los riesgos y proteger los activos.

   Las entidades gubernamentales deben implementar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada o maliciosa. Para esto deben realizar un análisis de riesgos que incluya un inventario de los activos de sistemas de información actualizados, que considere el equipo, los programas y los datos. Todos los activos deben ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones.

En particular, los datos electrónicos deben ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer lo que se va a proteger. Además, las evaluaciones de riesgos son importantes porque ayudan a asegurar que todas las amenazas y vulnerabilidades sean identificadas y consideradas, y los riesgos principales atendidos, y que se tomen las decisiones adecuadas respecto a los riesgos que se aceptarán y los que se mitigarán mediante los controles de seguridad.

El 29 de marzo de 2019 la directora de Finanzas, Contabilidad y Presupuesto nos suministró el *Análisis de Riesgos* aprobado[7] por el director ejecutivo de la Autoridad. El examen realizado el 3 de julio de 2019 reveló que este tenía las siguientes deficiencias:

- No consideraba la aplicación ARCGIS que fue implementada en el 2015
- No incluía las medidas de control establecidas para proteger los activos de acuerdo con las posibles amenazas que pudieran presentarse
- No incluía la conclusión de la gerencia en respuesta a su evaluación de riesgos (aceptación, transferencia, reducción o asumir el riesgo).

Criterios

Lo comentado es contrario a lo establecido en la Sección A de la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16* y en el Capítulo 3.1, *Security Management*, del FISCAM.

Efecto

La situación comentada impide a la Autoridad estimar el impacto que los elementos de riesgos tendrían sobre sus equipos y sistemas críticos, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

[7] El documento fue aprobado por el entonces director ejecutivo, pero no indicaba la fecha de aprobación. Dicho funcionario ejerció su cargo del 2 de agosto de 2010 al 15 de diciembre de 2012.

Causas

La oficial principal de informática y el director ejecutivo atribuyeron la situación comentada a que en la OSI no contaban con el personal ni el tiempo necesario para actualizar el *Análisis de Riesgos*. Además, no se consideró la conclusión de la gerencia en la preparación de este.

Comentarios de la Gerencia

El director ejecutivo nos indicó lo siguiente:

> Aceptamos las recomendaciones y estaremos trabajando en las deficiencias señaladas. [*sic*]

Véanse las recomendaciones 1 y 2.a.

Hallazgo 2 - Falta de un centro alterno para la recuperación de las operaciones computadorizadas

Situación

a. 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 19 de junio de 2019, la Autoridad no había formalizado un acuerdo escrito para el uso de un centro alterno, en el que se pudieran restablecer los sistemas de información computadorizados.

   Una situación similar fue comentada en el *Informe de Auditoría TI-07-09* del 29 de mayo de 2007.

Criterio

La situación comentada es contraria a lo establecido en el Capítulo 3.5, *Contingency Planning*, del FISCAM.

Efecto

La situación comentada podría afectar las operaciones de la Autoridad y los servicios de los sistemas de información computadorizados, ya que no tendrían disponibles unas instalaciones para operar después de una

emergencia o 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 de los sistemas de información computadorizados.

Causa

La oficial principal de informática atribuyó las situaciones comentadas a que la Autoridad no cuenta con el presupuesto para establecer un centro alterno. **[Apartado b.]**

Comentarios de la Gerencia

El director ejecutivo nos indicó lo siguiente:

> El 15 de octubre de 2019, la Administración para el Desarrollo de Empresas Agropecuarias (ADEA), el Departamento de Agricultura (DA) y la Autoridad de Tierras de Puerto Rico (ATPR), firmaron el acuerdo Interagencial […] en donde se establece […], que el Data Center de ADEA y DA servirán de centro alterno y recuperación para el Data Center de la ATPR. Al día de hoy, se han realizado los preparativos necesarios para que los datos y el mantenimiento de los servidores, puedan estar sincronizados con el centro de recuperación. Al momento estamos validando los parámetros de seguridad, parámetros de velocidad y los tamaños de los resguardos [...]. [*sic*] **[Apartado a.]**

Véanse las recomendaciones 1 y 2.b.

Hallazgo 3 - Deficiencias relacionadas con los parámetros de seguridad configurados en el servidor principal

Situaciones

a. Los controles de acceso limitan y detectan los accesos inapropiados a los recursos de tecnología (datos, equipos e instalaciones), y los protege de modificación no autorizada, pérdida y divulgación. Estos controles incluyen tanto los lógicos como los físicos. Los controles de acceso lógico requieren que los usuarios se autentiquen, mediante el uso de contraseñas secretas u otros identificadores, para limitar los archivos y otros recursos a los que pueden acceder y las acciones que

pueden realizar. Las entidades gubernamentales son responsables de diseñar y mantener la seguridad de sus sistemas de información, por lo que deben asegurarse de lo siguiente:

- Establecer formalmente políticas de cuentas (políticas de las contraseñas y de control de cuentas) basadas en riesgos, y requerir su cumplimiento.
- Limitar los intentos para acceder al sistema con una contraseña errónea, para asegurar que esta no pueda ser descifrada.
- Establecer, en las políticas y los procedimientos de la entidad, criterios para identificar los eventos significativos del sistema que se deben registrar.

La OSI contaba con un servidor principal configurado como *primary domain controller,* mediante el cual se controlaba el acceso a los recursos de la red de la Autoridad. Al 29 de mayo de 2019, en este servidor había 76 cuentas de usuarios activas para acceder a la red.

El examen efectuado a los parámetros de seguridad definidos al 6 y 12 de junio de 2019 en el sistema operativo del servidor principal de la Autoridad, reveló lo siguiente:

1) Las políticas de control de cuentas (*Account Lockout Policy*) no se habían definido para establecer:

    a) Un término de, al menos, tres intentos de acceso sin éxito, para que el sistema inactive automáticamente las cuentas (*account lockout threshold*)

    b) El tiempo que debía permanecer la cuenta desactivada por intentos de acceso sin éxito (*account lockout duration*)

    c) El tiempo para reiniciar el conteo de intentos de acceso sin éxito (*reset account lockout counter after*).

2) Las políticas de auditoría (*Audit Policy*) no se habían definido para que el sistema produjera un registro cuando ocurrieran eventos, tales como:

   a) La solicitud al servidor para validar las cuentas de usuario (*audit account logon events*)

   b) La creación, modificación o eliminación de una cuenta o grupo de usuarios; el cambio de nombre o contraseña; y la activación o desactivación de una cuenta o grupo de usuarios (*audit account management*)

   c) El acceso al directorio de servicio (*audit directory service access*)

   d) La activación y desactivación de las cuentas (*audit logon events*)

   e) Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*audit policy change*)

   f) El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*audit system events*).

3) La opción de seguridad *(security options)* para requerir al usuario utilizar una contraseña para continuar con el uso de la red, luego de un período de inactividad *(amount of idle time before suspending session)* no se había definido.

4) La opción de seguridad para requerir desactivar automáticamente del sistema al usuario una vez venciera el término de acceso a los recursos de la red, previamente establecido *(force logoff when logon hours expire)* no se había activado.

5) Las políticas sobre privilegios asignados a los usuarios *(user rights assignment)* no se habían definido.

Situaciones similares a las mencionadas en el **apartado a.1)a), y 2)b), c), e) y f)** fueron comentadas en el *Informe de Auditoría TI-07-09*.

Criterios

Las situaciones comentadas son contrarias a lo establecido en las secciones C.1 y E.11 de la *Política ATI-003* de la *Carta Circular 140-16*.

Lo comentado en el **apartado a.1) y 2)** es contrario a lo sugerido en el Capítulo 3.2, *Access Control*, del FISCAM.

Las situaciones comentadas en el **apartado a.1)b) y 3)** son contrarias a lo sugerido en el Capítulo 4.1, *Application Level General Controls*, del FISCAM.

Efectos

Las situaciones comentadas pueden propiciar que personas no autorizadas accedan a información confidencial mantenida en los sistemas computadorizados y puedan hacer uso indebido de esta. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **apartado a.2)** impide a la Autoridad mantener un registro de los eventos inusuales o los problemas ocurridos en la red, que le permita a la oficial principal de informática tomar a tiempo las medidas correctivas o preventivas necesarias.

Causa

La oficial principal de informática atribuyó las situaciones comentadas a que no había revisado las opciones de seguridad del sistema operativo que fueron configuradas antes de que ella ocupara su puesto.

Véanse las recomendaciones 1 y 2.c.

Hallazgo 4 - Falta de utilización del formulario de solicitud de acceso a los sistemas de información

Situaciones

a. En junio de 2012, la Autoridad estableció la utilización de la *Solicitud de Acceso a los Sistemas de Información* para ingresar un usuario nuevo, asignarle los privilegios correspondientes, desactivarlo y modificar sus privilegios. El formulario incluía, entre otra

información, el nombre y el puesto del empleado o solicitante, los programas o las aplicaciones para las que solicitaba el acceso y la justificación para acceder a Internet. Además, requería la firma del empleado y de su supervisor, la aprobación del director del departamento que solicitaba, y la firma del director del área de sistemas de información para autorizar que se efectúe la creación y el mantenimiento de las cuentas de acceso.

Al 8 de julio de 2019, no se encontró, ni le fue suministrada a nuestros auditores, evidencia de las solicitudes de acceso a los sistemas de información utilizadas para lo siguiente:

1) Solicitar y autorizar la creación de las cuentas de acceso correspondientes a los siete usuarios que comenzaron a trabajar en la Autoridad, entre el 9 de enero de 2017 y el 16 de octubre de 2018, y que le asignaron una cuenta de acceso.

2) Solicitar la modificación de los privilegios otorgados a las cuentas de acceso correspondientes a dos de nueve usuarios que cambiaron de puesto entre el 3 de enero de 2017 y el 19 de enero de 2019.

3) Solicitar la cancelación de las cuentas de acceso correspondientes a 11[8] de 14[9] usuarios que cesaron sus funciones en la Autoridad entre el 1 de enero de 2017 y el 1 de diciembre de 2018.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la Sección I de las *Normas y Procedimientos para la Instalación y Configuración de la Red*; y en el Artículo VI, sección Seguridad Lógica, de las *Normas y Procedimientos del Departamento de Sistemas de Información*, donde se establece la utilización de la *Solicitud de Acceso a los Sistemas de Información*.

[8] La oficial principal de informática nos indicó que, para uno de estos usuarios, le notificaron verbalmente que había renunciado.

[9] Las renuncias de los restantes tres usuarios fueron notificadas mediante correo electrónico

Efectos

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar, modificar o cancelar los accesos y privilegios a los usuarios. Esto dificulta las revisiones periódicas de las autorizaciones de acceso. Además, puede afectar la integridad de la información registrada en las aplicaciones de la Autoridad.

Lo comentado en el **apartado a.2)** ocasionó que los usuarios de las cuentas mencionadas permanecieran con los privilegios otorgados para los puestos que anteriormente ocupaban a pesar de que no le eran requeridos para realizar sus funciones. Esto, a su vez, puede propiciar que accedan información confidencial y hagan uso indebido de esta, y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados. Esto, sin que se puedan detectar a tiempo para fijar responsabilidades.

Causa

Las situaciones comentadas se atribuyen, según la oficial principal de informática, a que los procedimientos para la administración y el control de las cuentas de acceso de la Autoridad habían surgido como un requerimiento de la auditoría anterior, pero nunca se pusieron en vigor.

Véanse las recomendaciones 1 y 2.d.

Hallazgo 5 - Falta de almacenamiento de los respaldos fuera de los predios de la Autoridad

Situación

a. Las copias de respaldo deben almacenarse en lugares físicamente seguros fuera del ámbito de procesamiento, y que cumplan con todos los estándares requeridos.

   La Autoridad contaba con 21 servidores, de los cuales 15 eran virtuales. La oficial principal de informática era responsable de los respaldos realizados de la información mantenida en los servidores de la Autoridad. Los respaldos se efectuaban en la aplicación Veeam Backup and Replication, donde estaba configurada la ejecución

automática de los mismos. Diariamente se realizaban respaldos incrementrales y se mantenían en el disco duro del servidor Veeam Backup.

La evidencia obtenida reveló que, al 19 de junio de 2019, no se mantenía copia de estos respaldos fuera de los predios de la Autoridad.

Criterios

La situación comentada es contraria a lo establecido en el Artículo VI, sección *Resguardo de Información* (*Backup*), de las *Normas y Procedimientos del Departamento de Sistema de Información*, y en el *Plan para el Manejo y Seguridad de los Resguardos* (*Backup*), donde se establece que los respaldos de información deben almacenarse fuera de la entidad.

Efecto

La situación comentada puede ocasionar que, en casos de emergencia, la Autoridad no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Causa

Esta situación se atribuye a que en la Autoridad no cuentan con el presupuesto para guardar los respaldos en un lugar seguro y distante de los predios de esta.

Véanse las recomendaciones 1 y 2.e.

Hallazgo 6 - Deficiencias relacionadas con los controles ambientales en el Área de Servidores, y falta de organización e identificación del cableado que conectaba a los equipos de comunicación de la Autoridad

Situaciones

a. Las entidades deben establecer controles ambientales para prevenir o mitigar los daños potenciales a las instalaciones y las interrupciones en los servicios. Estos controles incluyen detectores de humo, alarmas de fuego y luces de emergencia, entre otros. Además, los recursos que apoyan las operaciones críticas y funciones de una entidad, incluidos los componentes de la red, deben identificarse y documentarse.

En la OSI había un cuarto, en el cual se mantenían los servidores y los equipos principales de la red de comunicación de la Autoridad (Área de Servidores). Además, en la Oficina de Fincas Familiares y en el área de archivos inactivos de la Oficina de Recursos Humanos habían instalados dos *switches*[10], uno en cada oficina, que mantenían la conexión con las computadoras de la Autoridad.

Las inspecciones efectuadas el 15 de abril y el 30 de mayo de 2019 de los controles existentes en el Área de Servidores y en las áreas dónde se mantenían los *switches* revelaron lo siguiente:

1) Relacionado con los controles ambientales en el Área de Servidores:

   a) No había equipos para detección de humo ni alarmas de fuego

   b) Se almacenaban materiales de oficina, equipos en desuso y otros materiales inflamables

   c) Las luces de emergencia estaban fuera de servicio.

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

   Una situación similar fue comentada en el *Informe de Auditoría TI-08-02* del 9 de octubre de 2007.

Criterio

Las situaciones comentadas se apartan de lo establecido en el Capítulo 3.5 del FISCAM.

[10] Dispositivo que permite la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

Efectos

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

Lo comentado en el **apartado a.2)** impide a la OSI obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

Causas

La oficial principal de informática atribuyó las situaciones comentadas a lo siguiente:

- No había realizado las gestiones necesarias para proteger los equipos de sistemas de información computadorizados. **[Apartado a.1)]**
- No contaba con el personal ni las herramientas necesarias para organizar e identificar el cableado en el Área de Servidores y en las oficinas donde estaban ubicados dos *switches.* **[Apartado a.2)]**

Véanse las recomendaciones 1, y 2.f. y g.

RECOMENDACIONES

A la Junta de Gobierno de la Autoridad de Tierras de Puerto Rico

1. Ver que el director ejecutivo cumpla con la **Recomendación 2**, de manera que se corrijan y no se repitan las situaciones comentadas en este *Informe*. **[Hallazgos del 1al 6]**

Al director ejecutivo de la Autoridad de Tierras de Puerto Rico

2. Velar por que el director ejecutivo auxiliar ejerza una supervisión efectiva sobre la oficial principal de informática para que esta se asegure de lo siguiente:

    a. Revisar el *Análisis de Riesgos* de la Autoridad para que se consideren e incluyan en el mismo los aspectos indicados en el **Hallazgo 1**. Una vez revisado, lo remita para su aprobación y

vea que se verifique cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de la Autoridad. Esto, para asegurarse de que este documento se mantenga actualizado.

b. Realizar las gestiones necesarias para establecer un centro alterno, y asegurarse de que el mismo cuente con el equipo necesario para restaurar las operaciones críticas de los sistemas de información computadorizados, en caso de desastres o emergencias. **[Hallazgo 2]**

c. Evaluar las opciones correspondientes a las políticas de control de las cuentas de accesos (*Account Lockout Policy*) y de auditorías (*Audit Policy*), los parámetros de seguridad (*Security Option*) y los privilegios asignados a los usuarios (*User Rights Assigments*), y active las que considere necesarias de acuerdo con los riesgos y las amenazas de los sistemas de información de la Autoridad. **[Hallazgo 3]**

d. Implementar y divulgar a los funcionarios y empleados los procedimientos para la administración y el control de las cuentas de acceso de la Autoridad, y asegurarse de que cumplan con estos. **[Hallazgo 4]**

e. Realizar las gestiones necesarias que permitan mantener copias de los respaldos en un lugar seguro y fuera de los predios de la Autoridad. **[Hallazgo 5]**

f. Establecer los controles ambientales necesarios para corregir las situaciones indicadas en el **Hallazgo 6-a.1)**. Esto, de manera que se asegure de que los equipos computadorizados de la Autoridad se mantengan en lugares donde estén protegidos contra posibles daños causados por condiciones ambientales que puedan afectar su disponibilidad y rendimiento.

g. Establecer un plan de trabajo para que se identifique y se organice el cableado de los equipos de comunicación de la Autoridad. **[Hallazgo 6-a.2)]**

APROBACIÓN

A los funcionarios y a los empleados de la Autoridad, 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

AUTORIDAD DE TIERRAS DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

MIEMBROS PRINCIPALES DE LA JUNTA DE GOBIERNO DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Carlos A. Flores Ortega	Presidente	8 abr. 19	27 ago. 19
Hon. Manuel Laboy Rivera	Miembro [11]	8 abr. 19	27 ago. 19
Lcdo. Luis C. Fernández Trinchet	" [12]	1 ago. 19	27 ago. 19
Sr. Gerardo J. Portela Franco	"	26 abr. 19	31 jul. 19
Sr. Luis Burdiel Agudo	"	8 abr. 19	25 abr. 19
Lcdo. Omar J. Marrero Díaz	" [13]	30 jul. 19	27 ago. 19
Sr. José I. Santiago Ramos	"	15 jul. 19	29 jul. 19
Lcdo. Christian Sobrino Vega	"	8 abr. 19	14 jul. 19

[11] El Lcdo. Julio R. Benítez Torres fue el representante autorizado del secretario de Desarrollo Económico de Puerto Rico.

[12] El Lcdo. Rafael I. Rodríguez Nevares fue el representante autorizado del presidente del Banco de Desarrollo Económico para Puerto Rico del 8 de abril al 11 de julio de 2019.

[13] El Sr. Alfredo Guerra Estevanell fue el representante autorizado del director ejecutivo de la Autoridad de Asesoría Financiera y Agencia Fiscal de Puerto Rico.

ANEJO 2

AUTORIDAD DE TIERRAS DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Agro. Juan L. Rodríguez Reyes	Director Ejecutivo	8 abr. 19	27 ago. 19
Agro. Luis A. Torres Díaz	Director Ejecutivo Auxiliar	8 abr. 19	27 ago. 19
Sra. Sheila Ureña Santaella	Oficial Principal de Informática	8 abr. 19	27 ago. 19

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