Estado Libre Asociado de Puerto Rico

OFICINA DEL CONTRALOR

INFORME DE AUDITORÍA
OC-25-61

11 de marzo de 2025

Departamento de Hacienda
Área de Tecnología de Información

(Unidad 5250 - Auditoría 15691)

Período auditado: 10 de julio de 2023 al 31 de julio de 2024

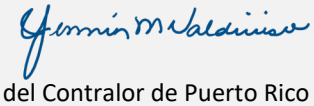
Finanzas Públicas

ÁREA DE FISCALIZACIÓN

Contenido

A los funcionarios y a los empleados del Departamento, 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.

Aprobado por:



Oficina del Contralor de Puerto Rico

Hicimos una auditoría de tecnología de información del Área de Tecnología de Información (ATI) del Departamento de Hacienda (Departamento) a base de los objetivos de auditoría establecidos; y 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*.

Este es el cuarto *Informe* y contiene dos hallazgos del resultado del examen que realizamos de los objetivos de auditoría. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

Opinión

Cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones del ATI y del Departamento objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con la ley y la reglamentación aplicable; excepto por los **hallazgos 1 y 2**.

Objetivos

General

Determinar si las operaciones del Departamento, en lo que concierne a los sistemas de información computadorizados se realizaron de acuerdo con la ley y reglamentación aplicables.

Específicos

1 - Evaluar los controles de acceso de las cuentas de usuario a la red de comunicación del Departamento conforme a lo establecido en las órdenes administrativas *18-15, Política General de Sistemas de Información*; *23-07, Política de Control de Acceso a los Sistemas de Información*; *OA 23-08, Enmienda a la Orden Administrativa*; *18-15, Política General de Sistemas de Información,* entre otras, para determinar lo siguiente:		
a. ¿Se limitan los accesos a la red, internos y remotos, y los privilegios de administrador conforme a las funciones realizadas por los usuarios?	No	**Hallazgos 1-a., b. y f., y 2-b.2)**

b. ¿Se informa oportunamente a la Oficina de Seguridad de Sistemas y Redes de Comunicación (Oficina de Seguridad) sobre la separación o transferencia de personal para la desactivación inmediata de estas?	No	**Hallazgo 1-c. al e.**
c. ¿Se mantiene documentación de la solicitud y autorización para la creación de las cuentas de acceso de los usuarios[1] de la red de comunicación, y esta incluye la información necesaria para evaluar los accesos solicitados?	No	**Hallazgo 2-a., b.1) y c.**
d. ¿Se configuran, en el servidor, las políticas de seguridad de las cuentas de acceso y se mantienen registros de auditoría?	Sí	No se comentan hallazgos
e. ¿Se mantiene un registro de los accesos de los usuarios a la red de comunicación para determinar eventos inusuales relacionados con estos accesos?	Sí	No se comentan hallazgos

[1] Incluidos los usuarios internos, los genéricos y consultores y, los que tienen privilegios de acceso remoto y administrativos.

Hallazgos

1 - Deficiencias relacionadas con el mantenimiento de las cuentas de acceso a la red de comunicaciones

Criterios

Sección I y Apartados A.2, A.3, A.5, A.7 A.8. y C. 2. de la Sección II de la *OA 23-07*; Sección II. n. de la *OA 09-04;* las secciones 6., 7.1.2, 7.1.6, 7.2.4, 7.7.2, 7.7.3 y 7.7.4 de la *Política TI-PRITS-007* **[Apartados a. al f.]**

El ATI del Departamento debe proteger los equipos, infraestructura, aplicativos y la seguridad, confidencialidad y disponibilidad de los datos e información generadas y utilizadas en las unidades del Departamento. Como parte de los controles de sistemas de información que se establezcan con este fin, el personal del ATI debe asegurarse, de que:

- Se establezcan, aprueben y divulguen procedimientos para la creación, aprobación, activación, modificación, desactivación y eliminación de cuentas de usuarios.
- Se establezcan mecanismos para identificar apropiadamente al personal a quien se le otorgue privilegios de acceso a los sistemas de información, para que solo se otorgue el acceso necesario para realizar tareas, roles y funciones específicas que le sean designadas. Además, mecanismos para que se revisen los accesos otorgados en caso de cambio, se elimine o modifique cualquier acceso innecesario y se controle el uso de cuentas con acceso privilegiado.
- Exista una coordinación adecuada con la División de Licencias, adscrita a la Oficina de Nómina y Licencias del Área de Recursos Humanos y Asuntos Laborales del Departamento, para que estos informen oportunamente al ATI sobre la separación, transferencia, desvinculación del servicio o ausencia prolongada de un empleado o funcionario.
- Se informe al ATI sobre cualquier cambio o terminación de relación con vendedores, suplidores, socios, contratistas, proveedores de servicios y otros terceros de modo que los accesos sean manejados o eliminados de forma adecuada.
- Se establezcan mecanismos para revisar y validar anualmente los accesos y desactivar las cuentas de usuarios que no son utilizadas, las que están asignadas a usuarios inactivos o ex personal contratado, y aquellas que no estén alineadas con las necesidades y autorizaciones vigentes.

La Oficina de Seguridad del ATI[2] cuenta con la División de Redes de Comunicación (División de Redes) que es dirigida por el oficial de redes, quién responde directamente al secretario auxiliar del ATI. En la División de Redes, se mantiene la documentación relacionada con la creación de las cuentas de acceso a la red, proceso que es realizado por una coordinadora de apoyo técnico y tres consultores de esta División.

[2] El ATI, adscrito a la Oficina del Subsecretario, es dirigido por un secretario auxiliar y responde a un oficial ejecutiva gubernamental que dirige el Centro de Excelencia Operacional del Departamento.

Al 3 de octubre de 2023, el Departamento contaban con 2,789 cuentas de acceso activas. De estas, 130 estaban asignadas a usuarios de otras agencias y 2,659 a usuarios del Departamento que incluían: empleados, empleados de otras agencias que laboraban en destaque o movilidad, consultores o contratistas, cuentas de servicio o genéricas, entre otros. Además, al 12 de julio de 2024, el Departamento tenía 26 grupos administrativos creados en el *Active Directory*.

Nuestro examen realizado sobre el mantenimiento de las cuentas de acceso del Departamento reveló que:

a. Al 6 de junio de 2024, una oficinista I de la Oficina del Secretario Auxiliar del ATI no pudo identificar los usuarios de 24 cuentas de acceso activas que no estaban incluidos en las listas de:
   - empleados del Departamento actualizada al 3 de octubre de 2023
   - consultores y contratistas provistas por el Departamento entre el 20 y 23 de febrero de 2024
   - usuarios de otras agencias provistas el 18 de marzo de 2024.

   Al 9 de julio de 2024, la secretaria auxiliar del Área de Recursos Humanos y Asuntos Laborales tampoco pudo identificar estos 24 usuarios y tres adicionales[3].

b. Al 12 de julio de 2024, había 9 grupos que tenían asignados privilegios administrativos que no eran utilizados por el Departamento y no se habían removido de las 23 cuentas de acceso activas que los tenían asignados. Estos privilegios estaban relacionados con la administración de la seguridad de los sistemas, los antivirus y la captura de planillas, entre otros.

Efectos

Permite que personas no autorizadas puedan lograr acceso a la red de comunicaciones del Departamento para hacer uso indebido de esta. También propicia la comisión de irregularidades; y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información. Esto, sin que pueda ser detectado a tiempo para fijar responsabilidades. **[Apartados a. al f.]**

Permite reducir la efectividad de los sistemas computadorizados, y exponer los datos y al personal a riesgos innecesarios que afecten la continuidad de las operaciones del Departamento. **[Apartado b.]**

Causas: El oficial de redes de la División de Redes informó que no se realiza un mantenimiento adecuado a las cuentas de acceso de la red de comunicaciones del Departamento y no existe un proceso de monitoreo automático que permita identificar las cuentas de acceso que no han sido utilizadas por más de 90 días. **[Apartados del a. al c. y f.]**

Atribuimos la situación comentada en el **Apartado a.** a que el formulario *Acceso al LAN* no requería incluir la clasificación del usuario para facilitar su identificación. **[Hallazgo 2-c.]**

Además, las cuentas de acceso de los grupos comentados no fueron desactivadas luego de que se cumpliera el propósito de la creación del grupo y su asignación a estas. **[Apartado b.]**

[3] Ocho de estos 27 usuarios se comentan en el **Apartado f.**

c. Del examen realizado del estatus y accesos de 15 cuentas de acceso de exempleados, que cesaron sus funciones entre el 31 de marzo de 1998 y el 30 de septiembre de 2023, determinamos que:

- Al 6 de junio de 2024, no se habían desactivado 4 cuentas de acceso de exempleados que cesaron sus funciones entre el 3 diciembre de 2015 y el 9 de abril de 2024.

  A dicha fecha habían transcurrido entre 58 y 3,108 días desde la separación de estos exempleados.

- Al 6 de junio de 2024, 4 cuentas de acceso inactivas que estaban asignadas a exempleados y 1 adicional que estaba activa, fueron utilizadas entre el 25 de marzo de 2023 y el 29 de mayo de 2024, esto luego del cese de las funciones.

  Habían transcurrido entre 29 y 9,125 días desde la separación de estos exempleados y la fecha de su último acceso. Estos cesaron funciones entre el 31 de marzo de 1998 y el 30 de septiembre de 2023.

Causas: La oficial en administración de recursos humanos principal de la División de Licencias indicó que notificaba anualmente al ATI de la separación de los empleados y terminación de trabajo en destaque y desconocía el requerimiento de la *OA 09-04* de notificar con regularidad al personal de las Oficina de Seguridad del ATI para la desactivación de las cuentas de acceso. **[Apartado c.]**

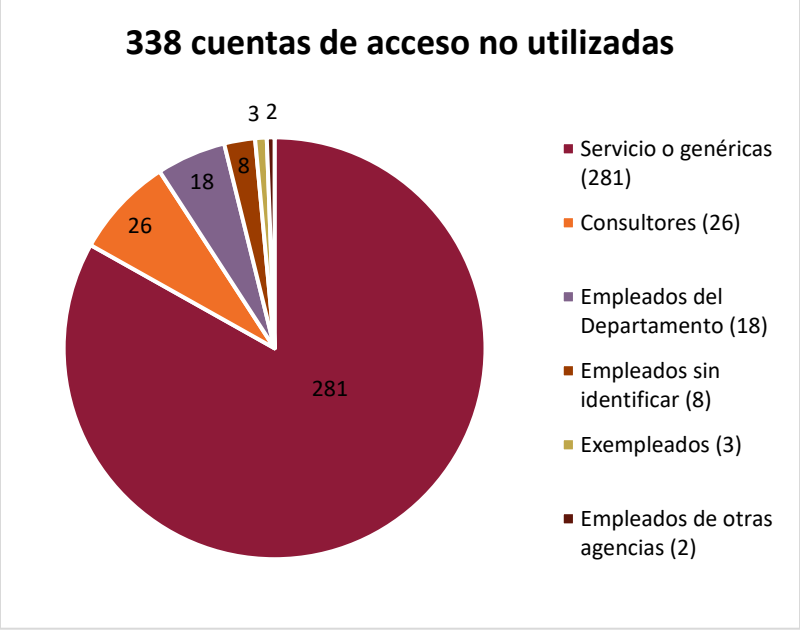
d. Al 3 de octubre de 2023, no se habían desactivado oportunamente 6 cuentas de acceso de empleados que iniciaron asignaciones en destaque en otras agencias entre el 1 de julio de 2021 y el 15 de septiembre de 2023. Habían transcurrido entre 18 y 824 días desde que había iniciado el destaque y la fecha de nuestro examen.

  A julio de 2024, los destaques de 2 de estos empleados se mantenían activos, 1 terminó el 16 de abril de 2024 y regresó a laborar en el Departamento y los otros tres destaques que habían vencido el 30 de junio de 2024 fueron extendidos hasta el 31 de diciembre de 2024.

e. Al 23 de agosto de 2024, determinamos que no se desactivó oportunamente la cuenta de acceso de un empleado que estaba en licencia desde el 16 de enero de 2024. La cuenta fue desactivada el 3 de julio de 2024, luego de transcurrido 169 días desde el inicio de esta licencia y la fecha en que desactivaron la cuenta.

Causas: El oficial de redes de la División de Redes indicó que la situación se debe a la falta de comunicación entre el Área de Recursos Humanos y Asuntos Laborales, y la Oficina de Seguridad para notificar aquellos empleados del Departamento que se encontraban en destaque o licencia para desactivar las cuentas de acceso asignados a estos. La oficial en administración de recursos humanos principal de la División de Licencias nos indicó que, las notificaciones de separaciones de empleo realizadas al ATI se llevan a cabo una vez al año. **[Apartados d. y e.]**

f. Al 3 de octubre de 2023, existían 338 cuentas de acceso que no se habían utilizado para acceder a la red de comunicaciones del Departamento durante un período mayor de 90 días y no habían sido desactivadas. El último acceso de estas cuentas ocurrió entre el 11 de marzo de 2010 y el 4 de julio de 2023. A la fecha de nuestro examen, habían transcurrido entre 91 a 4,953 días desde el último acceso. Estas cuentas incluían:



Recomendaciones 1.a.1) al 3) y 3.a.

2 - Deficiencias relacionadas con la creación de las cuentas de acceso a la red de comunicación del Departamento, las autorizaciones de acceso remoto y los formularios de solicitud de acceso

Criterios

Sección I. y apartados C.3, C.4., J.1 y J.5 de la Sección II de la *OA 23-07*, los artículos 7(a)(1), y 9 (a)(1) al (2) y (4) y 16(c)(1) del *Reglamento del Trabajo a Distancia*, las secciones 7.2.3, 7.2.5 y 7.5.1 de la *Política TI-PRITS-007* y el Capítulo 3.1 y 3.2, *Access Controls*, del *FISCAM*

El ATI debe mantener registros detallados de las transacciones que afectan perfiles de seguridad, los cuales deben ser archivados para auditorías. Además, debe utilizar formularios estandarizados que documenten la solicitud, recomendación, autorización y concesión o modificación del acceso concedido y contar con instrucciones claras para la autorización y gestión de cuentas.

En cuanto al acceso remoto, el ATI debe asegurarse de que se cumpla con el proceso establecido para otorgar este acceso y mantener documentación de las acciones realizadas tales como las solicitudes por escrito y su autorización, otorgar los accesos remoto según la necesidad, contar con la aprobación del secretario auxiliar de tecnología[4], y revisar periódicamente estos accesos para determinar si son apropiados. Además, el *Reglamento del Trabajo a Distancia* establece que el Área de Recursos Humanos y Asuntos Laborales debe evaluar las unidades y la elegibilidad de los empleados para teletrabajar y debe suscribirse un acuerdo por escrito entre el empleado y el Departamento. Para cualificar, los empleados interesados deben solicitar voluntariamente participar, su puesto debe ser adecuado para el teletrabajo y debe ser autorizado por el supervisor o director de la unidad.

Al 1 de mayo de 2024, existen 88 clases de puestos autorizados para este fin que están incluidos en la *Lista de Clases Elegibles para realizar Teletrabajo* (*Lista de clases*). Los empleados interesados deben completar el formulario *DH-RHAL0 21.1, Solicitud de Teletrabajo - Plan Piloto* (*Solicitud de Teletrabajo*) para solicitarlo.

El Departamento utiliza el *Formulario de Petición de Acceso al LAN* (*Acceso al LAN*) para solicitar los accesos a la red de los usuarios y el formulario *AS Form 1505, Information System Department System Access Request Form* (*formulario acceso remoto*) para solicitar los privilegios de acceso remoto. La documentación de las solicitudes y autorizaciones de las cuentas es custodiada por el personal de la División de Redes de la Oficina de Seguridad del ATI.

[4] En el Departamento, el secretario auxiliar de tecnología realizaba las funciones de un oficial principal de información (OPI) que incluyen gestionar la supervisión de la infraestructura tecnológica y el manejo de los datos.

Para el trámite de estas solicitudes se incluye la siguiente información:

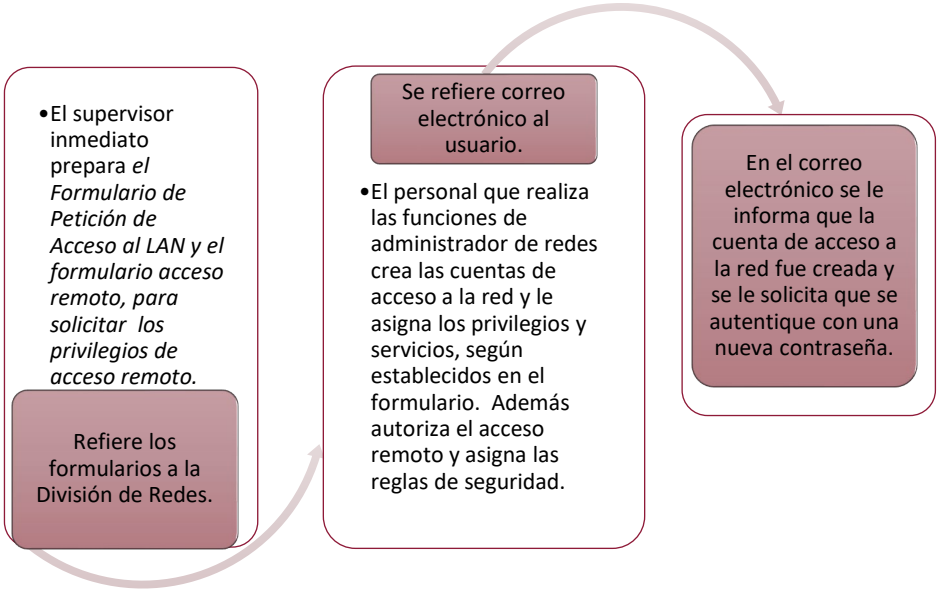
Acceso al LAN

- Nombre del peticionario y su información de contacto.
- Nombre del usuario e información de las aplicaciones, los privilegios de administrador y los servicios que deben ser asignados a su cuenta y su justificación.
- Acción solicitada (añadir, eliminar, modificar).
- Firma y fecha del peticionario y el pertonal del ATI.

formulario acceso remoto

- Información del usuario.
- Descripción del acceso requerido a nivel del firewall y otros servicios solicitados.
- Firmas y fecha del supervisor inmediato, y del director del ATI, entre otros.
- Código de identificación asignado al usuario y *token* asignado.
- La fecha de efectividad y expiración del acceso otorgado.
- El grupo de la red virtual privada.
- Información de la determinación del personal del ATI que otorga o deniega el acceso.
- La firma, fecha y hora de la firma del personal del ATI que otorga el acceso, entre otros.

El procedimiento para la solicitud de acceso a la red y remoto incluye los siguientes procesos:



Los formularios que son remitidos por correo electrónico se mantienen en la cuenta de correo del que solicita la creación de la cuenta de acceso, si la solicitud es enviada de forma física se archiva en un portafolio en la División de Redes de la Oficina de Seguridad.

Al 3 de octubre de 2023, el Departamento contaban con 2,789 cuentas de acceso a la red de comunicaciones que estaban activas.

a. Realizamos, entre el 9 de mayo y el 14 de junio de 2024, un examen de una muestra de 99[5] cuentas de acceso activas para determinar si el Departamento mantenía documentación que justificara la autorización y creación de estas, y los privilegios de accesos.

   En el examen de dichas operaciones encontramos que la Oficina de Seguridad no pudo suministrarnos documentación que justificara la creación de 79 cuentas y los 80 privilegios de acceso que tenían asignados. Una de estas cuentas tenía acceso a la red de comunicaciones y acceso remoto.

80 Privilegios No Documentados y Asignados a 79 Cuentas

Efectos

Impide al Departamento mantener la evidencia requerida para determinar si las cuentas de acceso y los privilegios otorgados están autorizados, y han sido asignado conforme a las funciones y los deberes de los usuarios. También puede propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta, la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información. Esto, sin que puedan ser detectados a tiempo para fijar responsabilidades.

[Apartados a. y b.]

Causas: El oficial de redes de la División de Redes informó que no contaban con un procedimiento que especificara los formularios que se deben utilizar para la solicitud y autorización de las cuentas y para la asignación de los privilegios, las instrucciones para cumplimentarlos, y el proceso de trámite y archivo de las solicitudes o formularios. Estos procedimientos no estaban incluidos en la OA 23-07. Además, indicó que el personal de la División de Redes no se aseguró de archivar la documentación de las solicitudes y autorizaciones de las cuentas al momento de crear las mismas. Esto, debido a que, en algunos casos, se perdió el tracto de la solicitud, lo que dificultó documentar el envío y recibo de esta. También estas cuentas habían sido creadas hace muchos años y en dos de los casos su documentación había sido extraviada.

[Apartados a., b.1) y c.]

[5] La muestra incluyó 28 cuentas de la red de comunicaciones (25 seleccionadas de forma aleatoria y 3 a juicio), 25 cuentas de servicio genéricas, 22 cuentas con privilegio de administrador y 25 cuentas con privilegio de acceso remoto. De estas 99 cuentas se evaluaron 100 privilegios de acceso debido a que había un empleado que contaba con el acceso a la red de comunicación y el privilegio de acceso remoto. Debido a esto contaba con dos formularios de solicitud de acceso.

b. Al 3 de octubre de 2023, el Departamento contaba con 1,004 cuentas de usuarios internos que tenían el privilegio para el servicio de acceso remoto. Seleccionamos una muestra de 25 cuentas de acceso que tenían acceso remoto **[Apartado a.]** para evaluar si se utilizó el *formulario acceso remoto*, si los puestos de estos usuarios correspondían a los autorizados para teletrabajo por el Área de Recursos Humanos y Asuntos Laborales y si los accesos eran necesarios conforme a entrevistas con los supervisores. El examen realizado entre el 14 de junio y el 17 de julio de 2024, reveló que:

1) Para 12 cuentas de acceso en las que nos proveyeron el *formulario acceso remoto* determinamos que:

a) En el formulario no se incluyó la información completa de la solicitud y la autorización del acceso, según se indica:

Información requerida	**Cantidad de formularios que no incluían la información**	**Porcientos**
Fecha de efectividad	8	67%
Descripción breve	5	42%
Otros servicios: Acceso Solicitado: acceso remoto, acceso inalámbrico, permiso de Internet, acceso para agencia externa, solicitud de IP público	3	25%
Firma del Usuario	1	8%
Firma de autorización del director del ATI o su representante autorizado	10	83%
Fecha de autorización del director del ATI o su representante autorizado	12	100%

b) En el formulario utilizado para 2 de estas cuentas de acceso el nombre del supervisor no era legible.

2) Once[6] cuentas de acceso estaban asignadas a empleados que según la *Lista de Clases* no estaban autorizados a realizar teletrabajo. La supervisora de 2 de estos empleados nos informó que no realizaban funciones que requerían acceso remoto.

Causas: El oficial de redes, en coordinación con personal de la Oficina de Seguridad, tiene pendiente la validación de los usuarios que deben permanecer con acceso remoto a través de la red privada local (*VPN*, por sus siglas en inglés). Esta tarea no se ha podido llevar a cabo debido al alto volumen de contratistas que requieren trabajar de forma remota. Además, la situación comentada se debe a la falta de monitoreo periódico sobre la actividad de uso de las cuentas de acceso y a que este privilegio no se restringe por un período de tiempo determinado. **[Apartado b.2)]**

Efectos

Esto, puede ocasionar errores en la autorización y creación de cuentas y en la asignación de privilegios de acceso que no estén relacionados con las tareas que realicen los usuarios correspondientes. Además, la falta de información necesaria en los formularios de autorización y creación de cuentas de acceso puede propiciar el riesgo de mal manejo, alteraciones o malentendidos en el proceso. **[Apartado c.]**

c. Al 26 de junio de 2024, el formulario *Acceso al LAN* y el *formulario acceso remoto* no incluían información necesaria para facilitar las revisiones de las solicitudes y autorizaciones de acceso, según se indica:

1) El formulario *Acceso al LAN* no incluía una sección para documentar si el acceso solicitado era para un usuario interno, externo o contratista. Además, no requería el puesto del usuario ni un formato uniforme en los campos de fechas de caducidad y de fecha de las firmas del peticionario y el personal de la ATI.

2) El *formulario acceso remoto* no requería un formato uniforme para las fechas que el supervisor solicita el acceso ni incluía una sección para documentar el nivel de acceso o grupos de Internet solicitado y otorgado al usuario. Entre estos: Usuarios Internet (Low), Usuarios Internet (Medium), Usuarios Internet (High) y Usuarios Internet (Streaming).

Recomendaciones 1.a.1) y 3) a la 5), 2 y 3.b.

[6] Para cinco de estas cuentas no presentaron el *formulario acceso remoto* y se comentan en el **Apartado a.** Además, para 4 de estas cuentas los supervisores informaron que debían tener acceso remoto.

Recomendaciones

Al secretario de Hacienda

1. Impartir instrucciones a la asesora técnica principal del Centro de Excelencia Operacional, para que se asegure de que el secretario auxiliar del ATI:
   a. Ejerza una supervisión efectiva al oficial de redes de la División de Redes de la Oficina de Seguridad para asegurarse de:
      1) Evaluar las cuentas mencionadas en los **hallazgos 1 y 2-b.2)** para actualizar los privilegios de acceso conforme a las funciones realizadas por los usuarios, e inhabilitar aquellas que no son necesarias para acceder a la red de comunicación del Departamento.
      2) Identificar los grupos administrativos a los que pertenecen las cuentas y removerlas de aquellos que no se utilizan. **[Hallazgo 1-b.]**
      3) Establecer revisiones periódicas de las cuentas de acceso a la red de comunicación del Departamento para evitar que se repitan las situaciones mencionadas. **[Hallazgos 1 y 2-b.2)]**
      4) Requerir la documentación para la solicitud y autorización para la creación de las cuentas de acceso. Asegurarse de que la documentación sea uniforme e incluya la información requerida que permita identificar al personal que solicita el acceso, previo a la autorización y asignación del privilegio de acceso a la red y acceso remoto. Además, mantener archivadas las solicitudes utilizadas para la asignación del privilegio de acceso remoto. **[Hallazgo 2-a. al b.1)]**
      5) Revisar los formularios de acceso para asegurarse de que: **[Hallazgo 2-c.]**
         a) El formulario *Acceso al LAN* requiera información que identifique la clasificación del usuario para el cual se solicita el acceso, el puesto del usuario; y requiera el uso de un formato uniforme de las fechas de caducidad y de las firmas del peticionario y personal del ATI. Además, evaluar el formulario para que incluya y requiera información actualizada.
         b) El *formulario acceso remoto* requiera un formato uniforme para la fecha de efectividad de los privilegios solicitados y otorgados y, documentar los niveles de acceso o grupos de Internet solicitados y otorgados al usuario. Además, evaluar el formulario para que incluya información actualizada.
2. Revisar y remitir para su aprobación, la *OA 23-07* para que incluya lo siguiente: los formularios que se utilizan para la solicitud y autorización de las cuentas, y la asignación de privilegios; las instrucciones para cumplimentar estos formularios; y el proceso de trámite y archivo de las solicitudes o formularios. Una vez se apruebe, asegurarse de que se mantenga actualizada. Además, orientar a los secretarios auxiliares del Departamento, para que estos se aseguren de que el personal supervisor cumpla con lo establecido en la *OA 23-07*. Esto, incluye completar y tramitar los formularios *Acceso al LAN* y *formulario acceso remoto* requeridos para la creación de cuentas y asignación de privilegios. **[Hallazgo 2]**
3. Impartir instrucciones a la secretaria auxiliar del Área de Recursos Humanos y Asuntos Laborales para que se asegure de que:
   a. La oficial en administración de recursos humanos principal de la Oficina de Asuntos Administrativos notifique inmediatamente al personal del ATI de las transacciones de personal tales como separación de empleo, licencias prolongadas, destaque o movilidad, para la desactivación oportuna de las cuentas de acceso. **[Hallazgo 1-c. al f.]**
   b. Evalúe y actualice el registro de las clases de puesto elegibles para el trabajo a distancia conforme las funciones de los empleados y las necesidades operacionales del Departamento. **[Hallazgo 2-b.2)]**

Información sobre la unidad auditada

El Departamento fue creado en virtud del Artículo IV, Sección 6, de la Constitución del Estado Libre Asociado de Puerto Rico. El Departamento tiene la responsabilidad de administrar la política pública relacionada con los asuntos contributivos y financieros; y la administración de los recursos públicos.

El Departamento es dirigido por un secretario nombrado por el gobernador con el consejo y consentimiento del Senado de Puerto Rico. Con el propósito de establecer las funciones generales del Departamento, y las facultades y funciones del secretario, el 22 de junio de 1994 se aprobó el *Plan de Reorganización 3-1994*, según enmendado. El secretario es responsable de coordinar y supervisar la administración de los programas y las funciones del Departamento y de sus componentes operacionales; aprobar los reglamentos a ser adoptados por los componentes del Departamento; y desarrollar e implementar normas y procedimientos de aplicación general al Departamento, entre otros. Además, delegará en funcionarios o empleados del Departamento, poderes, facultades, deberes o funciones que le hayan sido conferidos, excepto la facultad de adoptar o aprobar reglamentos, así como cualquier facultad indelegable por ley.

La misión del Departamento es elaborar y administrar las políticas tributarias y fiscales de forma justa, equitativa, ética, efectiva y eficiente, para promover el desarrollo económico del pueblo y educar sobre las mismas. Además, recaudar, custodiar, contabilizar y fiscalizar el uso de los recursos públicos por parte de las agencias gubernamentales para asegurar que se cumpla con las leyes y la reglamentación aplicable.

La estructura organizacional está compuesta por las oficinas del Secretario, Subsecretario y el Comisionado de Instituciones Financieras; las unidades asesoras que incluyen las oficinas de Apelaciones Administrativas; Asuntos Económicos y Financieros; Asuntos Legales; Comunicaciones; y el Centro de Excelencia Operacional; por las unidades de servicios auxiliares que incluyen las áreas de Administración[7], Recursos Humanos y Asuntos Laborales; Tecnología de Información; y por las unidades operacionales que incluyen las áreas de Finanzas Públicas[8]; Inteligencia de Fraude Contributivo; Política Contributiva; Rentas Internas; Seguros Públicos; el Centro de Servicio al Cliente; el Negociado de la Lotería de Puerto Rico; y la Oficina de Protección de los Derechos del Contribuyente.

El ATI, que es dirigido por un secretario auxiliar, es responsable de establecer las normas y políticas del uso de las tecnologías de informática; de planificar el desarrollo estratégico de los recursos técnicos y de programación; y de facilitar la administración del sistema contributivo del Gobierno. Además, provee los recursos y procedimientos tecnológicos y de programación de forma integral para todas las agencias del Gobierno Central, con el propósito de mantener el control, la contabilidad de los fondos y la propiedad pública.

La estructura organizacional del ATI está compuesta por: el Negociado de Tecnología de Información[9]; las oficinas de Administración; Desarrollo de Proyectos y Control de Calidad de Informática; y Seguridad de Sistemas y Redes de Comunicación (Oficina de Seguridad). Esta última oficina es responsable de administrar la seguridad lógica de los sistemas computadorizados de información y se divide en las divisiones de Seguridad de Sistemas y de Redes de Comunicación (División de Redes).

Los recursos para financiar las actividades operacionales del Departamento provienen principalmente de asignaciones especiales, fondos especiales estatales y de la resolución conjunta del presupuesto general.

El presupuesto asignado al Departamento, durante los años fiscales del 2022-23 al 2024-25, ascendió a $939,423,000 y $987,777,000, y $1,018,478,000, respectivamente.

[7] El Área de Administración estaba compuesta por las oficinas de: Administración de Instalaciones Físicas; Correspondencia y Conservación de Documentos Públicos; Finanzas; Presupuesto; y Servicios Generales.

[8] El Área de Finanzas Públicas estaba compuesta por los negociados de Contabilidad Central de Gobierno; y del Tesoro.

[9] El Negociado está compuesto por las divisiones de: Apoyo Técnico; Operaciones y Control; y Sistemas, Análisis y Programación. Al 20 de julio de 2023, el puesto de director del Negociado se encontraba vacante.

El **Anejo 1** contiene una relación de los funcionarios principales del Departamento que actuaron durante el período auditado. El Departamento cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: https://hacienda.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

Comunicación con la gerencia

Las situaciones comentadas en este *Informe* fueron remitidas al Lcdo. Nelson J. Pérez Méndez, entonces secretario del Departamento de Hacienda, mediante cartas del 26 de agosto y del 28 de octubre de 2024. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas. Mediante cartas del 4 de septiembre, y del 7 de noviembre de 2024, el entonces secretario remitió sus comentarios, los cuales se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe* se remitió para comentarios del entonces secretario y del CPA Francisco A. Parés Alicea, exsecretario, mediante correos electrónicos del 11 de diciembre de 2024.

El entonces secretario remitió sus comentarios mediante carta del 23 de diciembre de 2024 e indicó lo siguiente:

> Luego de revisar el borrador del informe, destacamos que el Departamento de Hacienda (Departamento) ha tomado las medidas necesarias para atender los hallazgos identificados estableciendo un plan de trabajo y coordinando entre sus unidades una mejor comunicación para lograr mantener la actualización de las cuentas de acceso a los sistemas de información. Las acciones específicas las hemos ya compartido con su oficina en la contestación de la carta a la gerencia (CG5250-15691-02) con fecha del 7 de noviembre de 2024. [*sic*]

Sus comentarios fueron considerados en la redacción final de este *Informe*.

El exsecretario Parés Alicea no remitió sus comentarios.

Control interno

La gerencia del Departamento 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 Departamento.

En los **hallazgos 1 y 2** se comentan las deficiencias de controles internos significativos, dentro del contexto de los objetivos de nuestra auditoría, identificada 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.

Alcance y metodología

La auditoría cubrió del 10 de julio de 2023 al 31 de julio de 2024. En algunos aspectos examinamos transacciones 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 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, empleados y consultores; exámenes y análisis de informes y de documentos generados por la entidad auditada; y pruebas y análisis de procedimientos de control interno y de otros procesos.

Para realizar esta auditoría utilizamos las órdenes administrativas *09-04 y 23-07*, el *Reglamento del Trabajo a Distancia* y la *Política TI-PRITS-007*, entre otros. Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica; el capítulo 3.2 del *FISCAM*. Aunque al Departamento no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas respecto a los controles y a la inversión en el campo de la tecnología de información.

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

Informes anteriores

El 7 de mayo de 2024 publicamos el *Informe de Auditoría OC-24-49* sobre el resultado del examen realizado de los controles para la continuidad de las operaciones y otros controles generales, relacionados con las operaciones de los sistemas de información computadorizados del Departamento y del Área de Tecnología de Información. Además, el 8 de julio de 2024 publicamos el *Informe de Auditoría OC-25-02* sobre el resultado del examen realizado sobre la implementación del sistema *Enterprise Resource Planning PeopleSoft v9.2*; y el 17 de octubre de 2024 publicamos el *Informe de Auditoría OC-25-31* sobre el resultado de los controles para la entrada de datos del Sistema de Ingresos y Recaudos del Área del Tesoro (SIRAT). Los mismos están disponibles en nuestra página en Internet.

Anejo 1 – **Funcionarios principales de la entidad durante el período auditado**

NOMBRE	PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Nelson J. Pérez Méndez	secretario[10]	1 feb. 24	31 jul. 24
CPA Francisco A. Parés Alicea	"	10 jul. 23	31 ene. 24
Lcdo. Nelson J. Pérez Méndez	subsecretario[11]	30 ene. 24	8 jul. 24
Hon. Ángel L. Pantoja Rodríguez	"	10 jul. 23	15 ene. 24
Lcdo. Josué R. Cardona Hernández	secretario auxiliar de Administración	10 jul. 23	31 jul. 24
Sra. Siris I. Báez González	oficial ejecutivo gubernamental del Centro de Excelencia Operacional	1 feb. 24	31 jul. 24
"	asesora técnica principal de la Oficina del Secretario[12]	10 jul. 23	31 ene. 24
Sr. José A. Rivera Mieles	secretario auxiliar del Área de Tecnología de Información[13]	16 feb. 24	31 jul. 24
Sr. Raúl A. Cruz Franquí	"	10 jul. 23	7 ene. 24
Sra. Jennifer M. Medina Meléndez	secretaria auxiliar del Área de Recursos Humanos y Asuntos Laborales[14]	23 jul. 24	31 jul. 24
Sra. Christie D. Machín Ramírez	"	10 jul. 23	18 jul. 24

[10] Ocupó el puesto de secretario interino del 1 de febrero al 8 de julio de 2024.

[11] Este puesto estuvo vacante del 16 al 29 de enero y del 9 al 31 de julio de 2024.

[12] Desde este puesto de confianza dirigía el Centro de Excelencia Operacional durante este período.

[13] Este puesto estuvo vacante del 8 de enero al 15 de febrero de 2024.

[14] Este puesto estuvo vacante del 19 al 22 de julio de 2024.

Anejo 2 – Definiciones

TÉRMINO	DEFINICIÓN
Acceso con Privilegio de Administrador	Se refiere a privilegios elevados destinados a realizar tareas legítimas de administración, como la instalación de actualizaciones y *software* de aplicación, administración de cuentas de usuarios, configuración de aplicaciones y modificación al sistema operativo, entre otros. Las cuentas con este privilegio deben contar con documentación e instrucciones formales para la autorización de este privilegio. Esto incluye la creación, asignación, uso y eliminación de dichas cuentas con capacidades elevadas.
Acceso remoto	Acceso que se origina desde las redes externas a la del Departamento.
Cuentas genéricas	Cuenta de acceso que no le corresponde a un usuario en particular. Puede utilizarse por un grupo de personas.
Cuentas de servicio	Cuentas de acceso utilizadas para brindar apoyo al contribuyente, recibir comunicaciones por correo electrónico sobre convocatorias, adiestramientos o seminarios a empleados de otras agencias, entre otros. La persona encargada o consultor que ofrecerá el curso es quien solicita la creación de estas cuentas.
Destaque o movilidad	Proceso para atender con flexibilidad las iniciativas del Gobierno. Esto, con el fin de identificar los recursos humanos necesarios que permitan la adecuada prestación y continuidad de los servicios que se le ofrece a la ciudadanía y que, a su vez, propician la mejor utilización y retención de los recursos humanos.
Legacy	Programa que ha llegado a su fin de vida. Esto se refiere a que ya no se provee mantenimiento ni realizan actualizaciones.
Red Privada Local (VPN)	Una red privada segura que utiliza servicios de telecomunicaciones públicas.

Fuentes legales

Leyes

Ley 184-2004. *Ley para la Administración de los Recursos Humanos en el Servicio Público del Estado Libre Asociado de Puerto Rico*, según enmendada. 4 de febrero de 2017.

Plan de Reorganización 3-1994. Plan de Reorganización del Departamento de Hacienda, según enmendado. 22 de junio de 1994.

Reglamentación

GAO 09-232 (2009). [Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos]. *Federal Information System Controls Audit Manual* (*FISCAM*). Febrero de 2009.

Reglamento del Trabajo a Distancia. (2020). [Departamento de Hacienda]. 31 de agosto de 2020.

Órdenes Administrativas

Orden Administrativa 09-04. (2009). [Departamento de Hacienda]. *Procedimiento para Someter Renuncias*. 9 de marzo de 2009.

Orden Administrativa 23-07. (2023). [Departamento de Hacienda]. *Política de Control de Acceso a los Sistemas de Información*. 24 de agosto de 2023.

Carta circular

Política TI-PRITS-007. [Puerto Rico Innovation and Technology Service]. *Política de gestión de acceso, identidad y credenciales V1.0*. 24 de enero de 2024.

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

Dichos principios se incluyen en la Carta Circular OC-18-19 del 27 de abril de 2018 y este folleto.

QUERELLAS

Apóyenos en la fiscalización de la propiedad y de los fondos públicos.

1-877-771-3133 | (787) 754-3030, ext. 2803 o 2805

querellas@ocpr.gov.pr

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente, por correo o teléfono o mediante correo electrónico. Puede obtener más información en la página de Internet de la Oficina, sección Queréllese.

INFORMACIÓN DE CONTACTO

105 Avenida Ponce de León Hato Rey, Puerto Rico

PO Box 366069 San Juan, Puerto Rico 00936-6069

(787) 754-3030 (787) 751-6768

www.ocpr.gov.pr ocpr@ocpr.gov.pr

SÍGANOS

Le invitamos a mantenerse informado a través de nuestra página de Internet y las redes sociales.

/ocpronline /ocpronline /contraloria_pr Prensa OCPR