

INFORME DE AUDITORÍA OC-24-49

26 de abril de 2024



Departamento de Hacienda
Área de Tecnología de Información
(Unidad 5250 - Auditoría 15606)

Período auditado: 30 de junio de 2018 al 31 de mayo de 2023

Contenido

OPINIÓN	2
OBJETIVOS	2
HALLAZGOS	4
1 - FALTA DE UN ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS	4
2 - FALTA DE ACTUALIZACIÓN DEL DISASTER RECOVERY PLAN GUIDE Y DE UN PLAN DE CONTINGENCIAS DEL ATI	5
3 - FALTA DE CONTROLES AMBIENTALES Y FÍSICOS EN EL CENTRO DE CÓMPUTOS, EN EL CUARTO DE TELECOMUNICACIONES Y EN LOS CUARTOS DE COMUNICACIONES	7
RECOMENDACIONES	11
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	12
COMUNICACIÓN CON LA GERENCIA	13
CONTROL INTERNO	13
ALCANCE Y METODOLOGÍA	14
ANEJO 1 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	15
ANEJO 2 - DEFINICIONES	16
FUENTES LEGALES	17

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 *Informe* contiene 1 hallazgo y 1 situación del resultado del examen que realizamos de los objetivos de auditoría; y 1 hallazgo y 1 situación de los controles internos. 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 del 1 al 3**.

Objetivos

General

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

Específicos

1 - Evaluar el cumplimiento del Artículo 3 de la <i>Ley 237-2004</i> , la <i>Ley Núm. 230</i> y la <i>Carta Circular 77-05</i> , para determinar si en el proceso de contratación y pagos de los servicios de respaldo, replicación, restauración de los datos del Departamento y el restablecimiento de sus operaciones en caso de emergencias:		
a. ¿Los contratos otorgados incluían todos los requisitos conforme a la reglamentación aplicables?	Sí	No se comentan hallazgos
b. ¿Se facturó y pagó por estos servicios conforme a la cuantía estipulada en los contratos otorgados y a la política pública establecida?	Sí	No se comentan hallazgos
c. ¿Se recibieron los servicios y beneficios según los contratos otorgados y la reglamentación aplicables?	Sí	No se comentan hallazgos

2 - Evaluar si el <i>Disaster Recovery Plan Guide (Plan)</i> , ¿está aprobado e incluye la información requerida para restablecer sus operaciones en caso de emergencia conforme a lo requerido en la Sección D. de la <i>Política ATI-015</i> y la Sección 7.2.10 de la <i>Política para la Seguridad Cibernética</i> y lo sugerido en el Capítulo 3.5, <i>Contingency Planning</i> , del <i>Federal Information System Controls Audit Manual (FISCAM)</i> ¹ ?	No	Hallazgo 2-a.
3 - Evaluar si el personal del ATI cumple con la <i>ATI-011</i> ² y la Sección H. de la <i>ATI-015</i> :		
a. ¿Se realizan pruebas al <i>Plan</i> para determinar si este asegura el restablecimiento de las operaciones del Departamento?	No	Hallazgo 2-a.
b. ¿Se asegura de que los centros alternos del Departamento funcionan adecuadamente y cuentan con los recursos necesarios (equipos, líneas de comunicación, sistemas, personal) para restablecer sus operaciones en caso de una emergencia?	No	Hallazgo referido al Departamento
4 - Evaluar si el personal de la División de Sistemas y Análisis y Programación se asegura de que el Centro de Cómputos cumple con las políticas <i>ATI-011</i> y <i>ATI-015</i> , en cuanto a lo siguiente:		
a. ¿Se respaldó con regularidad la información mantenida en los ambientes <i>mainframe</i> y cliente/servidor del Departamento?	Sí	No se comentan hallazgos
b. ¿Se mantenían copias de los respaldos de las aplicaciones críticas fuera de los predios del ATI del Departamento?	Sí	No se comentan hallazgos
c. ¿Se realizaron las pruebas de restauración de los datos críticos?	No	Hallazgo referido al Departamento

¹ El *FISCAM* está de acuerdo con las guías emitidas por el *National Institute of Standards and Technology*.

² Esta política fue derogada por la *Carta Circular 2023-004*. Además, en lo relacionado con los procesos de respaldos fue derogada por las políticas *TI-PRITS-004* y la *TI-PRITS-005*.

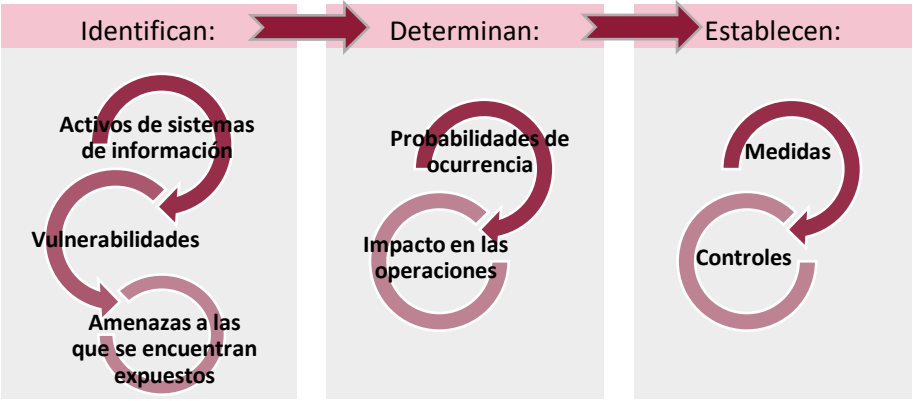
5 - ¿Se realizó el proceso de respaldo de los datos críticos del Sistema Unificado de Rentas Internas (SURI) hacia los centros alternos, conforme a los servicios contratados?	Sí	No se comentan hallazgos
6 - ¿Se establecieron controles ambientales y físicos en el Centro de Cómputos, el Cuarto de Telecomunicaciones y los cuartos de comunicaciones, conforme a lo establecido en la <i>Orden Administrativa 18-27</i> , el Artículo XIII del <i>Reglamento 11</i> , la Sección 2.1 de la <i>Política para la Seguridad Cibernética</i> y las secciones 3.5.3 y 3.5.16 de los <i>Estándares de Seguridad Cibernética</i> ?	No	Hallazgo 3

Hallazgos

1 - Falta de un análisis de riesgos de los sistemas de información computadorizados

Un análisis de riesgos es un proceso mediante el cual se:

Criterios
Sección C. de la *Política ATI-015*; y
Capítulo 3.1, *Security Management*, del
FISCAM



Esto, para evitar o disminuir los riesgos y proteger los activos, conforme a la clasificación establecida y el impacto en las operaciones.

El análisis de riesgos debe realizarse, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

El secretario auxiliar del ATI es el responsable de coordinar las tareas relacionadas con la evaluación y el manejo de los riesgos, y realizar el análisis de riesgos de los sistemas de información computadorizados del Departamento.

Nuestro examen reveló que, al 12 de abril de 2022, el Departamento no contaba con un análisis de riesgos.

Causas: El secretario auxiliar del ATI atribuyó esta situación a la falta de personal apto y con conocimiento en el tema. Además, el poco personal disponible en el ATI se concentraba en la resolución de los problemas causados por el impacto que habían tenido los incidentes tales como los terremotos, la pandemia, y los fallos en los acondicionadores de aire y del servicio de electricidad en las operaciones del Centro y el Cuarto de Comunicaciones.

Comentarios de la gerencia

Continuamente el equipo gerencial de ATI recibe el insumo en temas de seguridad cibernética de parte de los recursos asignados a la Oficina de Seguridad de Sistemas y Redes de Comunicación en temas de los activos, vulnerabilidades y amenazas. Se está trabajando para documentar el análisis de riesgos, en cuanto a las probabilidades de ocurrencia y el posible impacto.

Además, se documentarán las medidas y controles que se han estado ejecutando para reducir los riesgos que el equipo ha identificado.

—*secretario auxiliar de Administración*

2 - Falta de actualización del Disaster Recovery Plan Guide y de un plan de contingencias del ATI

- a. Un plan de recuperación de desastres se compone de las tareas, las actividades y los procedimientos formales que realiza la Unidad de Tecnología y Sistemas de Información, para el restablecimiento de los sistemas críticos de procesamiento de la agencia ante la eventualidad de un desastre o contingencia.

Este plan debe incluir las estrategias de respuesta, recuperación, reanudación y restauración para todos los procesos críticos de la agencia tanto a nivel de las plataformas de procesamiento como de sus comunicaciones. Las estrategias de continuidad establecidas por la agencia deben basarse en el *RTO* y el *RPO* de sus procesos críticos, establecidos en el informe de análisis de impacto.

Todas las agencias deben tener implementado, ejercitado y probado un plan de recuperación de desastres, el cual debe ser actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia, o cuando se realice un cambio significativo dentro de su infraestructura operacional.

El secretario auxiliar del ATI es el responsable de coordinar las tareas relacionadas con la preparación del plan de recuperación de desastres.

Efectos

El Departamento no pudo estimar el impacto que los elementos de riesgos tendrían sobre los sistemas de información, ni considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Recomendación 1.a.1) y 4), y b.

Criterio

Sección D. de la *Política ATI-015*

Efectos

Puede ocasionar que, en casos emergencias, el Departamento tome decisiones incorrectas y utilice de referencia procedimientos que no han sido probados y que no funcionan.

[Apartado a.]

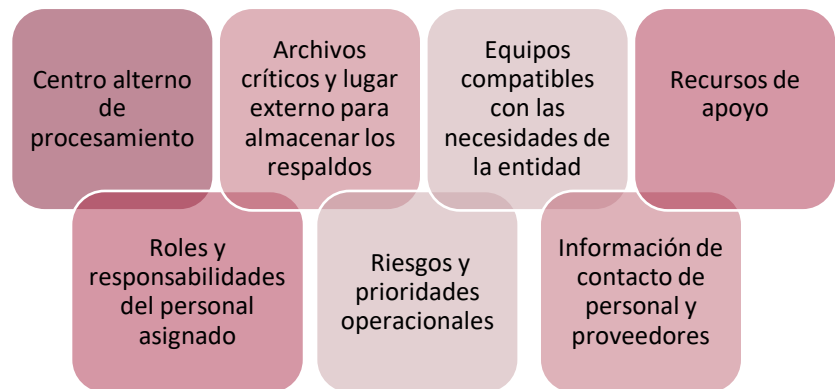
El examen realizado al *Disaster Recovery Plan Guide V. 2.0 (Plan)* reveló que, al 5 de octubre de 2022, no estaba actualizado.

Causa: El secretario auxiliar del ATI lo atribuyó a que no se habían autorizado horas adicionales en los contratos otorgados para este propósito.

Criterio
Capítulo 3.5 del *FISCAM*

- b. Toda entidad gubernamental debe contar con un plan de contingencias, para restablecer sus operaciones más importantes en caso de que surja una emergencia. Este debe incluir toda la información y los procesos necesarios para recuperar las operaciones de los sistemas de información computadorizados. También debe ser comunicado al personal responsable de las actividades de recuperación, y revaluado y probado bajo las condiciones que simulan un desastre.

Un plan de contingencias debe identificar:



El secretario auxiliar del ATI es responsable de coordinar las tareas relacionadas con la preparación del plan de contingencias.

Al 12 de abril de 2022, el secretario auxiliar del ATI nos proveyó el *Plan de Contingencia del Área de Tecnología de Información (Plan de Contingencia)* actualizado al 15 de marzo de 2022. Este *Plan de Contingencia* incluía los objetivos principales y establecía que la estrategia desarrollada por el Negociado para atender las contingencias debía considerar los generadores de energía disponibles, el personal con acceso remoto, el personal que debe acudir de forma presencial en caso de emergencia y el edificio principal del Departamento.

El examen realizado el 23 de agosto de 2022 al *Plan de Contingencia* reveló que este no detallaba la estrategia y no incluía información necesaria para atender las situaciones de emergencia.

Causas: El secretario auxiliar del ATI indicó que el personal del ATI no contaba con el conocimiento para la preparación de un plan de contingencias y desconocía sobre lo que este debía incluir. Esto, a pesar de que el personal del ATI conoce la importancia de la continuidad de las operaciones de los sistemas de información computadorizados del Departamento.

Efectos

Propicia la improvisación, y qué en casos de emergencias, se tomen medidas inapropiadas y sin orden alguno.

Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas en los servicios a los usuarios y clientes del Departamento. Además, pone en riesgo las operaciones contables, financieras y de nómina del Departamento y de las distintas agencias del gobierno.

[Apartados a. y b.]

Comentarios de la gerencia

Nos encontramos en proceso de actualización del *Disaster Recovery Plan Guide* del Departamento de Hacienda. Según mencionado anteriormente, con la aprobación de los fondos correspondientes, se comenzó el trámite de adquirir todos los componentes necesarios para la actualización física del DRS. Una vez esté todo instalado, configurado y se hayan realizado las pruebas aplicables, se trabajará con la actualización del plan de recuperación de desastres y el plan de contingencias de ATI. [...] **[Apartados a. y b.]**

—secretario auxiliar de Administración

Recomendación 1.a.2) al b.

3 - Falta de controles ambientales y físicos en el Centro de Cómputos, en el Cuarto de Telecomunicaciones y en los cuartos de comunicaciones

Las entidades deben establecer controles ambientales para prevenir o mitigar los daños potenciales a las instalaciones, e interrupciones en los servicios. Estos controles incluyen sistemas de supresión de incendios, alarmas de fuego, detectores de humo y agua, acondicionadores de aire y luces de emergencias.

También las instalaciones deben estar ubicadas en áreas seguras donde sea menor la posibilidad de daños por fuego, inundaciones y otros desastres; y contar con controles de acceso físico para que solamente personal autorizado pueda utilizarlas.

Además, todo activo fijo que se recibe debe numerarse y marcarse; y los recursos tecnológicos que apoyan las operaciones críticas y funciones de una entidad, incluidos los componentes de la red, deben identificarse y documentarse.

El ATI cuenta con el Centro, un Cuarto de Telecomunicaciones, y 16 cuartos de comunicaciones donde se mantienen los equipos principales de procesamiento y de la red de comunicaciones del Departamento.

El mantenimiento de la infraestructura física del edificio principal del Departamento es responsabilidad de la administración de la Autoridad de Edificios Públicos (AEP).

El personal de la División de Apoyo Técnico del ATI es responsable de mantener los controles ambientales y físicos del Centro, el Cuarto de Telecomunicaciones y los cuartos de comunicaciones³. Además, deben tramitar las solicitudes de servicio al oficial ejecutivo II de la Oficina de Administración de Instalaciones Físicas y Seguridad, para que sean referidas a la AEP.

Las inspecciones efectuadas el 6 y 12 de septiembre de 2022 de los controles ambientales existentes en el Centro y el Cuarto de

Criterios

Capítulo 3.5 del *FISCAM*
[Apartados a. y b.]

Artículos XI y XIII del *Reglamento 11*
[Apartado b.7)]

³ Como parte de los cambios efectuados en la estructura organizacional del ATI por la Reforma del Servicio Público, esta responsabilidad fue asignada al personal de la Oficina de Seguridad de Sistemas y Redes de Comunicación.

Telecomunicaciones; y el 16 de septiembre y 11 de octubre de los controles ambientales y físicos en 14 de los 16 cuartos de comunicaciones⁴, revelaron las siguientes deficiencias:

- a. El Centro, el Cuarto de Telecomunicaciones y los cuartos de comunicaciones tenían las siguientes deficiencias relacionadas con controles ambientales:

- 1) En el piso falso⁵ del Centro había áreas descubiertas, y en el del Cuarto de Telecomunicaciones había cables de data y eléctricos que no se utilizaban.

Efectos

Puede ocasionar daños y deterioros prematuros a los equipos de la red, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos y puede afectar la continuidad de los servicios provistos por el Departamento. También dificulta el mantenimiento de las áreas y de la red, y que se maximice el espacio disponible para estos equipos. **[Apartado a.]**

Causas: El supervisor de operaciones de tecnología de información del Negociado indicó que el Departamento no contaba con remplazos de este material para que fueran instalados en esta área. Además, el oficial ejecutivo II de la Oficina de Administración de Instalaciones Físicas y Seguridad del Área de Administración, indicó que el personal del ATI no había tramitado una solicitud para la compra de este material. El coordinador de apoyo técnico del ATI indicó que los cables no se habían removido debido a la falta de personal de la División de Apoyo Técnico, y a la falta de coordinación entre el personal de la División de Apoyo Técnico y la AEP para realizar estos trabajos. **[Apartado a.1)]**

- 2) Se mantenían equipos y materiales almacenados y otros en desuso, según se indica:
- a) En el Centro se mantenía 1 caja de discos de almacenamiento y 2 armarios de seguridad que pertenecían a una corporación que proveía servicios al Departamento y estos armarios llevaban entre 4 y 5 años sin utilizarse.
 - b) En el Cuarto de Telecomunicaciones se mantenían equipos tales como un panel de circuitos de comunicación, servidores y 6 armarios de seguridad con equipo, que no se utilizaba. Cuatro de estos armarios pertenecían al Departamento y 2 a una corporación. Los armarios de la corporación mantenidos en el Cuarto de Telecomunicaciones llevaban entre 4 y 5 años sin utilizarse.
 - c) En 9 cuartos de comunicaciones, se encontraron 13 equipos que se mantenían en los armarios de seguridad, los cuales no funcionaban y no habían sido removidos del área.
 - d) En 7 cuartos de comunicaciones, se almacenaban materiales tales como un abanico dañado, una bandeja plástica para llevar alimentos, cajas vacías, un carrito de carga, entre otros.

⁴ Nuestros auditores no pudieron inspeccionar 2 cuartos de comunicaciones.

⁵ Un piso que se coloca sobre otro para lograr un espacio entre estos. En el espacio logrado se permite las instalaciones eléctricas, el cableado estructurado y los drenajes.

Causas: En cuanto al equipo de la corporación, el secretario auxiliar del ATI lo atribuyó a la falta de coordinación para establecer el protocolo de recogido de estos equipos. El coordinador de apoyo técnico del Negociado indicó que los almacenes de propiedad del edificio del Departamento no contaban con espacio disponible para almacenar equipo adicional. Además, la oficinista II de la Oficina de Servicios Generales (OSG) indicó que el almacén en Trujillo Alto tampoco tenía espacio disponible para almacenar equipo y que los camiones para transportar el equipo al vertedero estaban dañados.

[Apartado a.2)]

- 3) En los plafones instalados en el techo del Centro observamos manchas de humedad causadas por la condensación de los conductos de las unidades de acondicionadores de aire.

Causa: El secretario auxiliar del ATI lo atribuyó a que la infraestructura física del edificio principal se encontraba deteriorada por la falta de mantenimiento continuo. **[Apartado a.3) al 5)]**

- 4) En 11 cuartos de comunicaciones la iluminación no era suficiente para que los técnicos del ATI o proveedores realizaran las tareas de mantenimiento.

Causa: El coordinador de apoyo técnico del Negociado y oficial ejecutivo II de la Oficina de Administración de Instalaciones Físicas y Seguridad lo atribuyeron a que los cuartos se construyeron para mantener los equipos que brindaban los servicios telefónicos y eléctricos, y no para el equipo de comunicaciones de la red. **[Apartado a.4) y 6)]**

- 5) En un cuarto de comunicaciones observamos filtraciones de agua en el techo. Durante nuestra inspección observamos un zafacón colocado encima del equipo de comunicación para evitar que este se mojara.

Causas: El cuarto de comunicaciones se encontraba debajo de un cuarto de baño que estaba fuera de uso y no se había realizado el mantenimiento a la tubería dañada. **[Apartado a.5)]**

- 6) En 6 cuartos de comunicaciones no se mantenía una temperatura adecuada para el funcionamiento del equipo.
- 7) En 12 cuartos de comunicaciones los equipos de comunicación se encontraban cubiertos de polvo.

Causa: No se realizaban inspecciones periódicas de los cuartos de comunicaciones por parte del personal de la División de Apoyo Técnico. Solo se inspeccionaban, cuando un usuario requería el servicio o en caso de interrupciones en las comunicaciones de la red del Departamento.

[Apartado a.7)]

Efectos

El personal de la División de Apoyo Técnico del Negociado no puede obtener una comprensión clara sobre los componentes autorizados de la red, de manera que se mantenga un control eficiente y efectivo para administrar y efectuar el mantenimiento de esta. Además, se dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente la conexión de nuevos equipos y mejoras de la red. **[Apartado b.1) al 4)]**

Efectos

No se mantiene un control adecuado de la propiedad y puede propiciar el uso indebido o la pérdida de esta, sin que se pueda detectar a tiempo para fijar responsabilidades. Además, dificulta la identificación y localización de los equipos. **[Apartado b.4)]**

- b. En los cuartos de comunicaciones tenían las siguientes deficiencias relacionadas con los controles físicos:

- 1) En 13 cuartos de comunicaciones el cableado que conecta los equipos de comunicación no estaba organizado.
- 2) En los 14 cuartos de comunicaciones el cableado que conecta a los equipos de comunicación no estaba identificado.

Causa: El coordinador de apoyo técnico lo atribuyó a que la División de Apoyo Técnico no contaba con el personal y las herramientas necesarias para organizar e identificar el cableado que conectaba el equipo que se mantenía en los cuartos de comunicaciones. **[Apartado b.1) y 2)]**

- 3) En los 14 cuartos de comunicaciones que mantenían los equipos de comunicación, no había un diagrama esquemático que ilustrara las conexiones autorizadas y establecidas con estos equipos.

Causas: El coordinador de apoyo técnico del Negociado atribuyó la situación a la falta de personal en la División de Apoyo Técnico y al crecimiento en las conexiones de los sistemas, debido al traslado de personal de otras oficinas al edificio principal del Departamento.

[Apartado b.3)]

- 4) En los 14 cuartos de comunicaciones se encontraron un total de 5 bandejas de fibra óptica y 91 paneles de conexión que no estaban identificados con número de propiedad.

Causa: La oficinista II de la OSG atribuyó la situación a que, en ocasiones, se otorgaban contratos por servicios que integraban la adquisición de equipo computadorizado y como parte del trámite de pago de este tipo de servicio, no se notificaba a la División de Propiedad para la identificación y el registro del equipo en el sistema Puerto Rico Integrated Financial Accounting System (PRIFAS). **[Apartado b.4)]**

Comentarios de la gerencia

[...] estamos en continua comunicación con la AEP para mejorar las instalaciones físicas del Departamento. Actualmente está en proceso una subasta pública cuyos trabajos permitirán la mejora de las situaciones indicadas en el informe, entre otras. [...] **[Apartado a.1) y 2)d) al 7)]**

[...] se está ejecutando un plan para el decomiso de equipo en desuso con nuestra Oficina de Servicios Generales y la Administración de Servicios Generales. Asimismo, se estableció un plan para que se retiren los equipos de proveedores anteriores y se numeren todos los equipos internos. [...] **[Apartados a.2)a) al c) y b.4)]**

[...] se logró la aprobación de fondos para la mejora de los cuartos de comunicaciones del edificio. Este proyecto se realizará por fases y ya se comenzó a trabajar en varios de los pisos del edificio. Esto mejorará los circuitos, la temperatura, [...], la organización del cableado y su identificación, entre otros. Al momento se han corregido los asuntos relacionados a iluminación, limpieza general [...].

[Apartado b.1) al 4)]

—*secretario auxiliar de Administración*

Recomendaciones 1.c. a la 3

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. Identifique alternativas costo-efectivas y se asegure de que se prepare, documente, revise el documento final y remita, para la consideración del secretario lo siguiente:
 - 1) Un análisis de riesgos que incluya los activos de los sistemas de información existentes, sus vulnerabilidades y amenazas, la probabilidad de ocurrencia y el impacto en las operaciones del Departamento, y las medidas y los controles necesarios para atender los riesgos asociados. **[Hallazgo 1]**
 - 2) Un plan de recuperación de desastres que incorpore los cambios significativos dentro de la estructura operacional y tecnológica del Departamento. Este plan debe ser probado antes de su aprobación para evaluar su efectividad. **[Hallazgo 2-a.]**
 - 3) Un plan de contingencias que incluya los requisitos necesarios para atender las situaciones de emergencia. **[Hallazgo 2-b.]**
 - 4) Una vez aprobados el análisis de riesgos y los planes, ver que se revisen cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Departamento, y asegurarse de que se mantengan actualizados. **[Hallazgos 1 y 2]**
 - b. Solicite, de ser necesario, asistencia operacional y técnica al Puerto Rico Innovation & Technology Service (PRITS), para que le oriente y apoye en la preparación del análisis de riesgos y los planes de recuperación de desastres y contingencias. **[Hallazgos 1 y 2]**
 - c. Solicite el personal y los recursos necesarios para que la División de Apoyo Técnico del ATI pueda ofrecer el mantenimiento al Centro, al Cuarto de Telecomunicaciones y los cuartos de comunicaciones. **[Hallazgo 3]**
Imparta instrucciones a este personal para que se asegure de:
 - 1) Instalar las losetas del piso falso en las áreas descubiertas del Centro. **[Hallazgo 3-a.1)]**
 - 2) Remover los cables de data y eléctricos del Cuarto de Telecomunicaciones y corregir las situaciones de humedad en los plafones del techo del Centro. **[Hallazgo 3-a.1) y 3)]**
 - 3) Coordinar con la Oficina de Servicios Generales los servicios necesarios para reubicar el equipo y materiales almacenados y disponer de los que estén en desuso, que se encuentran en el Centro y en los cuartos de comunicaciones. **[Hallazgo 3-a.2)]**

- 4) Establecer un itinerario periódico para el mantenimiento preventivo y continuo de los cuartos de comunicaciones y asegurarse de que los equipos de comunicación de la red del Departamento se mantengan en lugares protegidos contra posibles daños causados por condiciones ambientales que puedan afectar su disponibilidad y rendimiento. **[Hallazgo 3-a.4) al 7)]**
 - 5) Establecer un plan de trabajo para que se identifique y se organice el cableado de los equipos de comunicación del Departamento. **[Hallazgo 3-b.1) y 2)]**
 - 6) Preparar y mantener actualizados los diagramas esquemáticos de la red. **[Hallazgo 3-b.3)]**
 - 7) Identificar los equipos de comunicaciones, incluidos los componentes de la red, según establecido en el *Reglamento 11*. **[Hallazgo 3-b.4)]**
2. Asignar el personal necesario al ATI para que realicen las tareas mencionadas en el **Hallazgo 3-a.1) y b.1) al 3)**.
 3. Impartir instrucciones al secretario auxiliar de Administración para que:
 - a. Establezca los controles ambientales y físicos en el Centro, el Cuarto de Telecomunicaciones y los cuartos de comunicaciones. Entre estos, adquirir las losetas del piso falso del Centro; adquirir las herramientas para organizar e identificar el cableado conectado al equipo que se mantiene en los cuartos de comunicaciones. **[Hallazgo 3-a.1), y b.1) y 2)]**
 - b. Coordine con el oficial ejecutivo II de la Oficina de Administración de Instalaciones Físicas y Seguridad para que atienda las situaciones relacionadas con la remoción de los cables de data y eléctrico localizados debajo del piso falso del Cuarto de Telecomunicaciones; la humedad causada por la condensación de los aires en el Centro, la falta de iluminación y las filtraciones de las tuberías. **[Hallazgo 3-a.1) y 3) al 5)]**

Información sobre la unidad auditada

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

El 22 de junio de 1994 se aprobó el *Plan de Reorganización 3-1994*, según enmendado, con el propósito de establecer las funciones generales del Departamento, y las facultades y funciones del secretario de Hacienda.

El Departamento es dirigido por un secretario nombrado por el gobernador con el consejo y consentimiento del Senado de Puerto Rico. 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.

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, Recursos Humanos y Asuntos Laborales, y Tecnología de Información; y por las unidades operacionales que incluyen las áreas de Finanzas Públicas, Inteligencia de Fraude Contributivo, Política Contributiva, Rentas Internas, Seguros Públicos, el Negociado de la Lotería de Puerto Rico, el Centro de Servicio al Cliente y la Oficina de Protección de los Derechos del Contribuyente.

El Departamento ofrece sus servicios mediante 4 centros de servicios 360, 20 colecturías, 7 oficinas de cobro, 9 oficinas de distrito, 4 porteadoras, 7 unidades administrativas y un Centro de Servicio Integrado.

El Área de Tecnología de Información es dirigido por el secretario auxiliar y, a pesar de estar adscrito a la Oficina del Subsecretario, le responde a la asesora técnica principal de la Oficina del Secretario. Esta área es responsable de establecer las normas y políticas del uso de las tecnologías de informática; planificar el desarrollo estratégico de los recursos técnicos y de

programación; y 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; las oficinas de Administración; Desarrollo de Proyectos y Control de Calidad de Informática; y Seguridad de Sistemas y Redes de Comunicación.

Al 16 de marzo de 2022, el Departamento contaba con 2 *mainframes*, 16 servidores físicos y 251 servidores virtuales, y 3,117 computadoras entre otros equipos computadorizados. Además, el Departamento tenía implementados y en producción 295 aplicaciones o sistemas que se utilizaban para realizar sus operaciones. De estas, el ATI participa en las operaciones de 40 de ellas.

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 aprobado para el Departamento, para los años fiscales del 2021-22 al 2023-24, ascendió a \$208,103,000; \$939,423,000; y \$987,777,000, respectivamente.

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 los hallazgos de este *Informe* fueron remitidas al CPA Francisco A. Parés Alicea, entonces secretario de Hacienda, mediante

cartas del 10 de febrero y 2 de junio de 2023. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 23 de febrero y 16 de junio de 2023, los Lcdos. Ángel L. Pantoja Rodríguez, entonces subsecretario; y Josué R. Cardona Hernández⁶, secretario auxiliar del Área de Administración, remitieron sus comentarios, los cuales se consideraron al redactar el borrador de este *Informe*.

Mediante correo electrónico del 29 de noviembre de 2023, remitimos el borrador de este *Informe* al entonces secretario. Además, le remitimos en este borrador 2 hallazgos y 4 situaciones adicionales⁷ que por razones de seguridad determinamos no incluir en este informe. El borrador de uno de estos hallazgos también fue remitido al Lcdo. Raúl Maldonado Gautier y a la CPA Teresita Fuentes Marimón, exsecretarios.

El secretario auxiliar de Administración contestó mediante carta del 14 de diciembre de 2023 y sus comentarios fueron considerados en la redacción final de este *Informe*.

Los exsecretarios Maldonado Gautier y Fuentes Marimón no contestaron.

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.

⁶ La carta a la gerencia fue recibida y contestada por el licenciado Cardona Hernández, debido a que la persona designada, el licenciado Pantoja Rodríguez, no se encontraba en el Departamento para recibir y contestarla.

⁷ Estas situaciones también le fueron remitidas en las cartas del 10 de febrero y 2 de junio de 2023.

En los **hallazgos⁸ 1 y 2-b.** se comentan deficiencias de controles internos, las cuales no son significativas para los objetivos de la auditoría, pero merecen que se tomen medidas 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.

Alcance y metodología

La auditoría cubrió del 30 de junio de 2018 al 31 de mayo de 2023. 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 contratistas; 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 otros procesos.

Para las áreas que no estaban consideradas en la *Ley 237-2004*, la *Ley 230*, las políticas establecidas en la *Carta Circular 140-16*, el *Reglamento 11*, la *Política para la Seguridad Cibernética* y los *Estándares de Seguridad Cibernética*, utilizamos como mejor práctica; los capítulos 3.1, 3.3 y 3.5 del *FISCAM*. Aunque al Departamento no se le requiere cumplir con dichas

guías, entendemos que estas representan las mejores prácticas respecto a los controles en el campo de la tecnología de información.

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

Además, evaluamos la confiabilidad de los datos obtenidos del sistema PeopleSoft v8.4, que contiene las transacciones de los pagos efectuados por el Departamento, del 1 de enero de 2018 al 30 de junio de 2023. Como parte de dicha evaluación, se entrevistó a un consultor y empleado con conocimiento del sistema y de los datos; realizamos pruebas electrónicas para detectar errores evidentes de precisión e integridad; y revisamos la documentación e información existente sobre los datos y el sistema que los produjo. Determinamos que los datos eran suficientemente confiables para efecto de este *Informe*.

⁸ Un hallazgo adicional fue referida al Departamento.

Anejo 1 - Funcionarios principales de la entidad durante el período auditado

NOMBRE	PUESTO	PERÍODO	
		DESDE	HASTA
CPA Francisco Parés Alicea	secretario ⁹	25 jun. 19	31 may. 23
Lcdo. Raúl Maldonado Gautier	"	25 feb. 19	24 jun. 19
CPA Teresita Fuentes Marimón	secretaria interina	1 ago. 18	27 ene. 19
Lcdo. Raúl Maldonado Gautier	secretario	30 jun. 18	31 jul. 18
Lcdo. Ángel Pantoja Rodríguez	subsecretario ¹⁰	25 jun. 19	31 may. 23
CPA Francisco Peña Montañez	"	4 mar. 19	24 jun. 19
Sr. Juan C. Puig Morales	" ¹¹	1 oct. 18	31 ene. 19
Lcda. Roxana Cruz Rivera	subsecretaria	30 jun. 18	15 sep. 18
Lcdo. Josué R. Cardona Hernández	secretario auxiliar de Administración	4 ene. 21	31 may. 23
Sra. Siris Báez González	secretaria auxiliar interina de Administración ¹²	9 dic. 20	3 ene. 21
Sr. Santiago A. Rosado Pabón	secretario auxiliar de Administración	8 may. 19	4 dic. 20
Sr. Orlando C. Rivera Berríos	"	30 jun. 18	7 may. 19
Sr. Raúl A. Franqui Cruz	secretario auxiliar del Área de Tecnología de Información ¹³	3 ago. 18	31 may. 23

⁹ Ocupó el puesto de secretario interino del 28 de enero al 24 de febrero, y del 25 de junio al 7 de julio de 2019.

¹⁰ Ocupó el puesto de subsecretario interino del 25 de junio de 2019 al 1 de diciembre de 2020.

¹¹ Este puesto estuvo vacante del 16 al 30 de septiembre de 2018, y del 1 de febrero al 3 de marzo de 2019.

¹² Este puesto estuvo vacante del 5 al 8 de diciembre de 2020.

¹³ Este puesto estuvo vacante del 30 de junio al 2 de agosto de 2018.

Anejo 2 - Definiciones

TÉRMINO	DEFINICIÓN
Centro alterno	Local escogido por la empresa para operar los servicios de TI en caso de que, por cualquier motivo, no pueda tenerse acceso a las instalaciones normales.
Cliente-servidor	Modelo en el que los clientes o usuarios están conectados a un servidor.
Infraestructura tecnológica	Incluye las plataformas, aplicaciones, redes y datos.
Mainframe	Computadoras de alto rendimiento con grandes cantidades de memoria y procesadores que procesan miles de millones de cálculos y transacciones simples en tiempo real.
Servidor	Es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.
Objetivo de punto de recuperación (RPO)	Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable.
Objetivo de tiempo de respuesta (RTO)	Se refiere al tiempo durante el cual una organización puede tolerar la falta de funcionamiento de sus aplicaciones, sin afectar la continuidad del negocio.
Piso falso	Un piso que se coloca sobre otro para lograr un espacio entre estos. En el espacio logrado se permite las instalaciones eléctricas, el cableado estructurado y los drenajes.
Respaldo de datos	Proceso que consiste en crear una copia de los datos originales y almacenarlos en un dispositivo con el objetivo de recuperar la información durante alguna contingencia.
Replicación	Proceso que consiste en crear una copia exacta y actualizada a tiempo real de los datos de un dispositivo de almacenamiento primario a uno secundario. Esto, con el propósito de apoyar la disponibilidad y la recuperación de los datos ante un desastre.
Restauración	Proceso de copiar archivos de una copia de seguridad, generalmente un disco separado a la ubicación original u otras ubicaciones de archivo apropiadas para facilitar las operaciones adecuadas de las bases de datos.

Fuentes legales

Leyes

Ley 230, *Ley de Contabilidad de Gobierno de Puerto Rico*. 23 de julio de 1974.

Ley 237-2004, *Ley para Establecer Parámetros Uniformes en los Procesos de Contratación de Servicios Profesionales y Consultivos para las Agencias y Entidades Gubernamentales del ELA*. 31 de agosto de 2004.

Reglamentación

Reglamento 11 de 2005. [Departamento de Hacienda]. *Normas Básicas para el Control y la Contabilidad de los Activos Fijos (Reglamento 11)*. 29 de diciembre de 2005.

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.

Órdenes Administrativas

Orden Administrativa 18-27. (2018). [Departamento de Hacienda]. *Control de Acceso en Áreas que Trabajan con Información Contributiva Federal*. 4 de diciembre de 2018.

Cartas circulares

Carta Circular 77-05. [Oficina de Gerencia y Presupuesto]. *Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*. 8 de diciembre de 2004.

Carta Circular 140-16. [Oficina de Presupuesto y Gerencia]. *Normas Generales sobre la Implantación de Sistemas, Compra de Equipos, y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*. 7 de noviembre de 2016.

Carta Circular 2021-007. [Puerto Rico Innovation and Technology Service]. *Establecimiento de la Política para la Seguridad Cibernética*. 6 de diciembre de 2021.

Carta Circular 2023-004. [Puerto Rico Innovation and Technology Service]. *Normas Generales que deben seguir las agencias al establecer sus controles y procedimientos, de manera que se atiendan adecuadamente los recursos, las adquisiciones e implementación de soluciones o tecnología nueva, así como el uso y manejo de los sistemas de información y el manejo de cambios en los proyectos de tecnología*. 30 de junio de 2023.

Estándares de Seguridad Cibernética [Puerto Rico Innovation and Technology Service]. 29 de octubre de 2021.

Política ATI-015. [Oficina de Gerencia y Presupuesto]. *Programa de Continuidad Gubernamental*. 12 de octubre de 2016.

Política ATI-011. [Oficina de Gerencia y Presupuesto]. *Mejores Prácticas de Infraestructura Tecnológica*. 7 de noviembre de 2016.

Política para la Seguridad Cibernética, v.1.0. [Puerto Rico Innovation and Technology Service]. 29 de octubre de 2021.

Política TI-PRITS-004. [Puerto Rico Innovation and Technology Service]. *Política sobre los Servicios de Tecnología*. 30 de junio de 2023.

Política TI-PRITS-005. [Puerto Rico Innovation and Technology Service]. *Política sobre las Mejores Prácticas de Infraestructura Tecnológica*. 30 de junio de 2023.



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.