OFICINA de la CONTRALORA
GOBIERNO DE PUERTO RICO

INFORME DE AUDITORÍA
OC-26-34

27 de mayo de 2026

Administración de Vivienda Pública
Área de Sistemas de Información Tecnológica

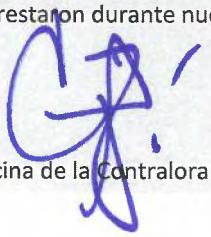
(Unidad 5331 – Auditoría 15767)

Período auditado: 1 de enero de 2022 al 4 de junio de 2025

Contenido

A los funcionarios y a los empleados de la Administración, 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 de la Contralora de Puerto Rico

Realizamos una auditoría de tecnología de información del Área de Sistemas de Información Tecnológica (ASIT) de la Administración de Vivienda Pública (Administración) 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 dos (2) hallazgos del resultado del examen que realizamos de los objetivos de auditoría; y cuatro (4) hallazgos de los controles internos. 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 de la Administración 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 6**.

Objetivos

General

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

Específicos

1 - Evaluar si se han establecido controles de acceso en el Yardi Voyager Housing Software (Sistema Yardi) conforme a lo establecido en las secciones 6.1.1, 6.1.6 y 6.2.3 de la *Política para la Seguridad Cibernética*, y las secciones 7.1.2, 7.1.7, 7.2.1, de la 7.2.3 a la 5, 7.2.7, 7.3.1.2, 7.4 y 7.7.3 de la *Política TI-PRITS-007* y de las secciones 3.2 y 3.4 del Capítulo 3 del *FISCAM*[1], entre otros, para determinar lo siguiente:		
a. ¿Se documentaron y se autorizaron los accesos otorgados a los usuarios del sistema que son empleados de la Administración?	No	**Hallazgo 1-a.**
b. ¿Existe segregación de deberes en los procesos de solicitud, autorización y administración de accesos al sistema?	Sí	

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

c. ¿Se otorgaron los privilegios de acceso de las cuentas activas conforme a las funciones que deben realizar los usuarios en el sistema?	Sí	
d. ¿Se desactivaron las cuentas de acceso que estaban asignadas a los exempleados de la Administración con acceso al sistema y estas no fueron utilizadas posterior a la renuncia o separación del puesto?	No	**Hallazgo 2-a.**
e. ¿Se desactivaron las cuentas de acceso del sistema no accedidas?	No	**Hallazgo 2-b.**
f. ¿Se configuran las políticas de seguridad de las cuentas de acceso relacionadas con el control de las contraseñas?	Sí	
g. ¿Se controla el uso de las cuentas de acceso con privilegio administrativo asignadas al personal de los agentes administradores?	No	**Hallazgo 1-b.**
2 - Evaluar los datos registrados en el Sistema Yardi para determinar si, conforme a lo establecido en la Sección 8 de la *Política TI-PRITS-005*, el *Reglamento 8624*, y las tablas límite de ingreso establecidas por el Departamento de Vivienda Urbana Federal (HUD por sus siglas en inglés), para determinar lo siguiente:		
a. ¿Se han establecido controles que garanticen la integridad y la confiabilidad de la información registrada de las familias beneficiarias del Programa de Vivienda Pública y de las listas de espera?	Sí	
b. ¿Se han establecido controles de procesamiento que garanticen la corrección de los procesos de cualificación y determinación de la renta?	Sí	

Hallazgos de otros asuntos surgidos	
• Informe de Análisis de Riesgos de los Sistemas de información	**Hallazgo 3**
• Programa de Ciberseguridad y Procedimientos para Responder a Incidentes de Seguridad	**Hallazgo 4**
• Plan de Contingencia y Plan de Recuperación de Desastres	**Hallazgo 5**
• Políticas y Procedimientos Relacionados con las Operaciones de los Sistemas de Información	**Hallazgo 6**

Hallazgos

1 - Deficiencias relacionadas con la documentación de las cuentas de acceso del Sistema Yardi

a. Las agencias deben documentar y registrar adecuadamente la creación de cuentas de usuario y las modificaciones de accesos.

Además, deben establecer un proceso para informar estas autorizaciones, que incluya el uso de formularios estandarizados, para reducir el riesgo de mal manejo, alteraciones o malentendidos. Estos formularios deben mantenerse archivados.

La Administración utiliza el sistema Yardi Voyager Housing Software (Sistema Yardi) que es un servicio de suscripción donde se administran: todos los proyectos de vivienda pública, incluidos los procesos desde el mantenimiento de la unidad hasta la asignación de la vivienda; el Programa de Sección 8; y las demás operaciones de la agencia. Además, en este sistema se mantiene información confidencial relacionada con la composición familiar, la condición económica y las circunstancias particulares presentadas por los solicitantes de estos programas.

Para la creación de las cuentas de acceso se utiliza el *Formulario Solicitud de Acceso Sistema Voyager - Yardi (Formulario)* que incluye la información oficial del usuario, el tipo de usuario y de empleado, y su estatus laboral. Además, para documentar el acceso a la red requiere que se detalle lo siguiente:

- Tipo de solicitud que incluye entre éstas los encargados de trabajar los casos, de realizar inspecciones o las órdenes de servicio.
- Lista de propiedades a las que debe tener acceso el usuario, que incluye el código y nombre de la propiedad.
- Órdenes de Compra que detalla las acciones que realizará el usuario relacionadas con las órdenes de compra y cuentas por pagar.

El proceso de solicitud, creación, mantenimiento de cuentas de usuarios es el siguiente:

- **Solicitud -** El supervisor completa la parte de *Acceso a la Red* del *Formulario* y lo remite para la aprobación de la administradora auxiliar.
- **Creación -** La administradora auxiliar del ASIT verifica que el *Formulario* esté debidamente completado y envía un correo electrónico a la compañía consultora para la creación de la cuenta de usuario de acuerdo con los accesos y los roles solicitados por el supervisor.

El empleado recibe un correo electrónico con una contraseña genérica, acompañado de las instrucciones a seguir para activar la cuenta y cambiar la contraseña.

- **Cambios -** De surgir algún cambio en el puesto del empleado, el supervisor debe enviar un correo electrónico a la administradora auxiliar del ASIT para notificar sobre el cambio de puesto del empleado y de los accesos y de los roles que deben ser modificados al usuario.

  La administradora auxiliar, le envía un correo electrónico al gerente de sistemas de información para efectuar los cambios de los accesos.

Al 31 de diciembre de 2024, existían 374 cuentas de acceso de empleados que estaban activas en el sistema Yardi. De estas, identificamos 62 que fueron creadas entre el 3 de enero de 2022 al 12 de diciembre de 2024[2] y seleccionamos una muestra de 25 cuentas. El examen realizado de los formularios de acceso utilizados para la autorización de las 25 cuentas seleccionadas reveló que no incluían toda la información requerida, según se indica:

Información requerida en la solicitud	**Cantidad de solicitudes que no incluían la información**
Código o Nombre de Propiedad	1
Orden de Compra/Cuentas a Pagar	22
Tipo de Solicitud	8
Tipo de Usuario	4
Tipo de Empleado	2

b. Las agencias deberán contar con documentación e instrucciones formales para la autorización y la gestión de cuentas con privilegios de administrador o acceso especial. Esto incluye la creación, asignación, uso y eliminación de dichas cuentas con capacidades elevadas.

Al 31 de diciembre de 2024, el Sistema Yardi utilizaba grupos de seguridad con el propósito de mantener una segregación de la disponibilidad de la información que podía ser accedida y controlar las acciones que podían ser realizadas por cada usuario. Entre estos:

- Un grupo de seguridad[3] que estaba asignado a los empleados de la compañía de consultores y al equipo de la ASIT para la administración de las cuentas de acceso y de la información de los participantes y propiedades registrados en el sistema Yardi. A la fecha de nuestro examen existían 16 cuentas de acceso activas que pertenecían a este grupo de seguridad.
- Un grupo de seguridad[4] asignado a las cuentas de acceso de los encargados de los sistemas de información de los agentes administradores para la administración de las cuentas de acceso, ver información relacionada con el agente administrador que tiene asignada la cuenta y, acceder y modificar información de los participantes de los proyectos de vivienda pública asignados. A la fecha de nuestro examen existían 36 cuentas de acceso activas que pertenecían a este grupo de seguridad.

[2] Para identificar estas 62 cuentas, se extrajo de las 374 cuentas activas las creadas desde el 1 de enero de 2022 al 31 de diciembre de 2022.

[3] Este grupo de seguridad era el *Super-Administrator*.

[4] Este grupo de seguridad era el *7ma_admi* y tenía un rol tipo subadministrador.

El examen de estas cuentas reveló que, al 4 de junio de 2025 la administradora auxiliar del ASIT no contaba con la documentación relacionada con la autorización para la creación de estas cuentas asignadas a los grupos de seguridad.

Criterios

Las situaciones comentadas son contrarias a las siguientes disposiciones:

- Sección 7.2.3 de la *Política TI-PRITS-007* **[Apartado a.]**
- Capítulo 3.2, *Access Controls*, del *FISCAM* **[Apartado a.]**
- Sección 7.2.5 de la *Política TI-PRITS-007* **[Apartado b.]**

Efectos

Las situaciones comentadas tienen los siguientes efectos:

- Impide a la Administración 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. **[Apartado a.]**
- Impide a la Administración mantener un control efectivo de la asignación y uso de las cuentas de acceso con los privilegios administrativos. Además, propicia a que se otorguen accesos no autorizados y, lo que, aumenta la posibilidad de comisión de irregularidades sin que puedan detectarse a tiempo para fijar responsabilidades. **[Apartado b.]**

Causas

Las situaciones identificadas responden, entre otras cosas, por lo siguiente:

- La administradora auxiliar del ASIT atribuyó la situación a que este formulario fue creado por el Área de Finanzas y Administración específicamente para las cuentas de los usuarios de los agentes administradores, y la información de los roles y las opciones de "workflows" no fueron modificado antes de comenzar a utilizarlo en la oficina central. Al no estar actualizado, los administradores asociados o supervisores completan el formulario mediante comentarios acorde a las funciones similares que realiza otro empleado que tiene acceso. Además, nos indicó que debido a la falta de recursos en el ASIT se le ha dificultado completar la actualización de los procedimientos para controlar el acceso lógico. **[Apartado a.]**
- La administradora auxiliar del ASIT nos certificó que no mantiene documentación de la creación de estas cuentas debido a que se crearon desde la conversión. En ese entonces, la ASIT no tenía a su cargo el proyecto de implementación del Sistema Yardi. **[Apartado b.]**

Recomendaciones 1 y 3.a. a la c.

Comentarios de la gerencia

> Se está trabajando con la creación de varios formularios con la programación correspondiente de los diferentes grupos de seguridad para cada área administrativa tanto para los empleados de la AVP (Oficina Central y Regiones) y otro para el personal de los agentes administradores. De esta manera podemos tener segregados los accesos y tener mejores controles de seguridad. [*sic*]
>
> –*director ejecutivo*

2 - Falta de inactivación de las cuentas de acceso al Sistema Yardi asignadas a exempleados y no utilizadas

a. Las agencias están obligadas a implementar los procedimientos necesarios para garantizar que tanto las personas como los sistemas obtengan únicamente el acceso necesario a los recursos para realizar sus tareas y funciones específicas. En situaciones de separación, desvinculación del servicio o ausencia prolongada de un empleado o funcionario, el departamento de recursos humanos debe notificar de inmediato al oficial principal de informática[5] (OPI). El OPI deberá restringir la cuenta y los accesos de forma inmediata. Además, la agencia es responsable de establecer los procesos necesarios para informar al OPI, o al empleado designado por este, sobre cualquier cambio o terminación de relación con terceros, de modo que los accesos sean manejados o eliminados de forma adecuada.

La Secretaría de Recursos Humanos del Departamento de la Vivienda (Departamento), a través de un acuerdo colaborativo, maneja las transacciones de Recursos Humanos de la Administración. El proceso interno utilizado para el manejo de las separaciones de empleados incluye:

- **Secretaría de Recursos Humanos del Departamento** - Entrega al supervisor del funcionario el formulario *DV-SRHSA-67, Certificación Propiedad no Fungible*, para que notifique los equipos que debe entregar a la Administración.
- **Administradora auxiliar del ASIT** - Recibe el formulario. Verifica si el empleado tiene que entregar equipo de sistemas de información y certifica el recibo de este. Además, las cancelaciones de cuentas de acceso las puede solicitar el supervisor vía llamada telefónica a la administradora auxiliar del ASIT.

  La administradora auxiliar del ASIT envía un correo electrónico al gerente de sistemas de información para que este proceda con la cancelación de los accesos.

Realizamos una comparación entre la lista certificada de exempleados de la Administración[6] provista el 4 de marzo de 2025 por la secretaria auxiliar interina de Recursos Humanos del Departamento. La lista está compuesta por 374 cuentas con estatus activo asignadas a empleados de la Administración en el Sistema Yardi al 31 de diciembre de 2024.

Nuestro examen reveló que, al 31 de diciembre de 2024, permanecían activas las cuentas de acceso de 23 exempleados que cesaron sus funciones, entre el 15 de julio de 2022 y el 15 de diciembre de 2024. Esto es entre 16 y 900 días desde la separación de estos exempleados.

El 7 de julio de 2025 la administradora auxiliar del ASIT informó que había inactivado estas cuentas de acceso.

b. Los controles de acceso se deben revisar periódicamente para garantizar su alineación con las necesidades y autorizaciones vigentes. Como parte de esta gestión, las cuentas de acceso que los usuarios no utilizan deben ser inactivadas y removidas de manera oportuna. La administradora auxiliar del ASIT es la encargada de coordinar y supervisar las actividades administrativas y operacionales en el ASIT. Entre estas, las relacionadas con el mantenimiento de las cuentas de acceso del Sistema Yardi.

[5] Es el empleado responsable de la gestión y supervisión de la infraestructura tecnológica y manejo de datos de una agencia. Estas funciones las realiza la administradora auxiliar del ASIT en la Administración.

[6] Esta lista incluye 84 empleados que tenían una fecha de separación del servicio del 15 de julio de 2022 al 31 de diciembre de 2024.

Al 31 de diciembre de 2024 existían 2,527 cuentas de acceso activas asignadas a empleados de la administración y usuarios externos con privilegios de acceso al Sistema Yardi. El examen realizado de estas cuentas de acceso activas reveló que 412[7] (16%) cuentas, no se habían utilizado para acceder al sistema por más de 90 días. Al 31 de diciembre de 2024, habían transcurrido desde 91 hasta 3,514 días desde su último acceso.

Criterios

Las situaciones comentadas son contrarias a las siguientes disposiciones:

- Secciones 6, 7.7.3 y 7.7.4 de *Política TI-PRITS-007* **[Apartado a.]**
- Sección 7.1.6 de la *PolíticaTI-PRITS-007* y el Capítulo 3.2, *Access Controls*, del *FISCAM* **[Apartado b.]**

Efectos

Las situaciones comentadas tienen los siguientes efectos:

- El no desactivar las cuentas de acceso de los exempleados permitió que en una cuenta se registrara un acceso posterior a la fecha de la renuncia del empleado. **[Apartado a.]**
- Impide a la Administración mantener un control efectivo y eficaz sobre las cuentas de acceso y asegurar que estas sean utilizadas solo por personas autorizadas a acceder la información confidencial mantenida en sus sistemas. **[Apartados a. y b.]**
- Dificulta fijar responsabilidad por el uso indebido y no autorizado de estas cuentas para acceder o alterar información confidencial de la Administración. **[Apartados a. y b.]**

Causas

Las situaciones identificadas responden, entre otras cosas, por lo siguiente:

- El administrador nos certificó que, al 7 de julio de 2025, la Administración no cuenta con un protocolo formalmente documentado. En su lugar, la agencia lleva a cabo un procedimiento interno para la desactivación de accesos cuando un empleado se desvincula de la agencia. Este proceso puede presentar demoras en su ejecución, lo cual puede generar riesgos relacionados con el control de accesos y la seguridad de la información. **[Apartado a.]**
- La administradora auxiliar del ASIT nos certificó que las revisiones de las cuentas no utilizadas no se realizan de manera ordinaria debido a que existe un problema con el envío del informe de cuentas sin actividad que produce la compañía consultora. **[Apartado b.]**

Recomendaciones 1, 2 y de la 3.d. a la g.

Comentarios de la gerencia

En el mes de julio se publicó el "Request for Proposal" AVP-RFP-24-25-03 "Management Agents Services" en el cual se establece lo siguiente: El Agente de Administración es responsable de gestionar la consola administrativa del correo electrónico corporativo para proteger toda la Información y el acceso a las diferentes aplicaciones utilizadas en la AVP.

[7] De estas 371 cuentas de acceso estaban asignadas a usuarios externos y 41 cuentas de acceso estaban asignadas a empleados de la Administración.

> […] las diferentes compañías se les brindo una orientación por cada una de las áreas administrativas y operaciones de la agencia […] En la cual al personal que trabaja todo lo relacionado a sistemas de información […], se le brindó el taller de la parte administrativa de las funciones y las responsabilidades. En la parte de la aplicación de Yardi para la asignación de los accesos que no estaba permitido el uso de cuentas comerciales […] que las cuentas a ser creadas […] serán cuentas individuales no pueden estar creadas cuentas con nombres de proyectos de vivienda pública corporativa […] De esta manera se mantiene un control de los empleados que laboran en los proyectos de vivienda pública y nosotros como empleados de la agencia. [*sic*]
>
> –*director ejecutivo*

3 - Falta de un informe de análisis de riesgo de los sistemas de información computadorizados

Un 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 se encuentran expuestos. Además, se establecen medidas de seguridad y controles adecuados para evitar o disminuir los riesgos y proteger los activos.

Cada jefe de agencia debe designar a una persona o equipo que será responsable del manejo de los riesgos de la entidad. El personal designado debe evaluar los riesgos y el impacto que podría resultar del acceso no autorizado, la utilización, la divulgación, la interrupción, la modificación o la destrucción de información de los sistemas de información, entre otros. Además, debe evaluar y manejar los riesgos en todos los activos y sistemas de información, y garantizar que la tolerancia al riesgo se refleje de la misma manera en toda la agencia. Este proceso debe ser documentado.

El examen realizado de dichas operaciones reveló que, al 26 de noviembre de 2024 la Administración no contaba con un informe del análisis de riesgos relacionado con sus sistemas de información computadorizados.

Criterios

La situación comentada es contraria a las siguientes disposiciones:

- Secciones 7.2, 7.2.2 y 7.2.11 de la *Política para la Seguridad Cibernética* y Capítulo 3.1, Security Management, del *FISCAM*.

Efectos

La situación comentada tiene los siguientes efectos:

- La Administración no puede estimar el impacto que los elementos de riesgos tienen sobre los sistemas de información utilizados, ni considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Causas

La situación identificada responde, entre otras cosas, por lo siguiente:

- La administradora auxiliar del ASIT nos certificó que se encontraban realizando varios cambios en la infraestructura de comunicaciones en el edificio central y en las oficinas regionales, por lo que se debe analizar cómo se impactarán las distintas áreas administrativas y operacionales de la Administración previo a realizar el análisis de riesgo.
- Además, informó que la Administración no cuenta con personal capacitado o con experiencia para preparar el análisis de riesgo y no se ha realizado la contratación de un recurso externo.

Recomendaciones 1 y 3.h.

4 - Falta de un programa de ciberseguridad y de procedimientos para responder a incidentes de seguridad

a. Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como, la privacidad y la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que estos puedan sentirse cómodos al acceder a dichas tecnologías.

Toda agencia, en colaboración con el Puerto Rico Information Technology Service (PRITS), debe desarrollar, documentar e implementar un programa de ciberseguridad. El programa como mínimo, debe incluir:

- Todos los activos de información de la Agencia, incluido los servicios de informática provistos por terceros.
- Una evaluación de riesgos de ciberseguridad que la Agencia lleve a cabo por lo menos una vez al año.
- Un plan educativo que vele por la educación del personal, los contratistas, y la ciudadanía, incluidos cursos especializados para el desarrollo de los administradores de sistemas y tecnologías sobre las mejores prácticas de ciberseguridad.
- Una evaluación de vulnerabilidades de seguridad tanto interna como externa para validar la efectividad de los controles que la agencia haya implementado.

La administradora auxiliar del ASIT es responsable de asesorar y ofrecer apoyo tecnológico y procesal al Administrador para la formulación de política pública que regirá al ASIT y a los representantes de las distintas áreas programáticas de la agencia.

Nuestro examen reveló que al 13 de enero de 2025 la Administración no había desarrollado, documentado o implementado un programa de ciberseguridad.

b. Cada jefe de agencia debe designar a una persona o equipo que será responsable de la seguridad cibernética de la agencia. Esta persona o equipo es responsable de desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad cibernética que incluyan los procesos de mitigación de los riesgos asociados con los incidentes antes de que se produzcan daños sustanciales; notificar y consultar al PRITS; y notificar y consultar con los organismos encargados de hacer cumplir la ley y otras oficinas, según corresponda.

El examen realizado de dichas operaciones reveló que al 4 de octubre de 2024 la Administración no contaba con un plan o procedimiento aprobado para el manejo de incidentes de seguridad relacionados con sus sistemas de información computadorizados.

Criterios

Las situaciones comentadas son contrarias a las siguientes disposiciones:

- Artículo 5 de la *Ley 40-2024* **[Apartado a.]**
- Secciones 7.2 y 7.2.9 de la *Política para la Seguridad Cibernética* **[Apartado b.]**

Efectos

Las situaciones comentadas tienen los siguientes efectos:

- Impide el desarrollo y el establecimiento de planes de respuesta dirigidos a evitar o mitigar los efectos reales o potenciales de ciberataques dirigidos a los sistemas de información computadorizados de la Administración. **[Apartado a.]**

- Propicia la improvisación y que, en casos de emergencia, se tomen las medidas inapropiadas y sin orden alguno. Además, puede ocasionar retrasos en el proceso de evaluación, contención, mitigación y erradicación y recuperación de los incidentes. **[Apartado b.]**

Causas

Las situaciones identificadas responden, entre otras cosas, por lo siguiente:

- La administradora auxiliar del ASIT nos certificó que no se ha implementado el programa de ciberseguridad debido a que el área no cuenta con el personal para realizar todos los procesos necesarios para su desarrollo. **[Apartado a.]**
- La administradora auxiliar del ASIT nos informó que no se ha desarrollado el procedimiento para el manejo de incidentes debido a que no han completado los cambios en la estructura tecnológica de la Administración y a la falta de recursos en el ASIT. **[Apartado b.]**

Recomendaciones 1 y 3.i.

---

5 - Falta de un Plan de Contingencia y de un Plan de Recuperación de Desastres

a. Un plan de contingencias de los sistemas de información debe incluir toda la información y los procesos necesarios para recuperar las operaciones principales de los sistemas de información computadorizados que se vean afectados durante una emergencia. También debe ser comunicado al personal responsable de las actividades de recuperación, y revaluado y probado bajo las condiciones que simulan una emergencia. Además, este plan debe identificar:
   - El centro alterno de procesamiento
   - Los archivos críticos y lugar externo para almacenar los respaldos
   - Los equipos compatibles con las necesidades de la entidad
   - Los recursos de apoyo
   - Los roles y responsabilidades del personal asignado
   - Los riesgos y prioridades y operacionales
   - La información de contacto de personal y proveedores.

   Las agencias deben desarrollar un plan de contingencia de acuerdo con la Política de Seguridad Cibernética y los Estándares para la Seguridad Cibernética para asegurar la continuidad de las operaciones de sus sistemas de información computadorizados.

   La administradora auxiliar del ASIT dirige y coordina las actividades operacionales que se desarrollan en la ASIT.

   El examen realizado reveló que al 4 de octubre de 2024 la Administración no contaba un plan de contingencia.

b. Un plan de recuperación de desastres es un plan escrito para procesar aplicaciones críticas en caso de un evento mayor que afecte el equipo, los programas computadorizados y destruya las facilidades de procesamiento. Provee los procedimientos para facilitar la recuperación en un centro alterno y estos deben ser probados.

   Las agencias son responsables de asegurar la continuidad de sus operaciones mediante un plan de recuperación de desastre desarrollado por la agencia, de acuerdo con la Política para la Seguridad Cibernética promulgada por el PRITS. Este plan abarcará todo lo relacionado a programación (software), equipo, (hardware), datos y facilidades físicas de la Agencia.

El examen realizado reveló que al 13 de enero de 2025 la Administración no contaba un plan de recuperación de desastres.

Criterios

Las situaciones comentadas son contrarias a las siguientes disposiciones:

- Sección 8.1.3 de la *Política TI-PRITS-005* y Sección 7.2.10 de la *Política para la Seguridad Cibernética* **[Apartado a.]**
- Capítulo 3.5, *Contingency Planning*, del *FISCAM* **[Apartados a. y b.]**
- Sección 7.2.4 de la *Política TI-PRITS-004* **[Apartado b.]**

Efectos

Las situaciones comentadas tienen los siguientes efectos:

- Las situaciones comentadas propician la improvisación y el uso de procedimientos no probados en casos de emergencias. Esto podría representar un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios ofrecidos a los usuarios de los sistemas de información computadorizados. **[Apartados a. y b.]**
- Puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno. **[Apartados a. y b.]**

Causas

Las situaciones identificadas responden, entre otras cosas, por lo siguiente:

- La administradora auxiliar de la ASIT nos certificó que no se han completado los planes de contingencia y recuperación de desastres debido a que la Administración ha estado trabajando en los pasados meses en unos cambios de configuración de la red que son bien significativos para las operaciones en el ASIT. Una vez completadas todas las fases de este proyecto, se comenzará con el desarrollo de estos planes y se realizarán los simulacros para probar los procedimientos establecidos. **[Apartados a. y b.]**

Recomendaciones 1 y 3.j.

6 - Falta de políticas y procedimientos relacionados con las operaciones de los sistemas de información computadorizados

Las agencias deben cumplir con las políticas de manejo de información y los estándares tecnológicos relativos a la informática emitidos por el PRITS. Para esto deben impartir instrucciones necesarias para asegurar su cumplimiento.

Además, la gerencia de cada agencia debe establecer un sistema de control interno efectivo. Para esto, debe diseñar, implementar y documentar las actividades de control relacionadas con los sistemas de información, y asegurarse que respondan a los riesgos y objetivos de la entidad. Estas actividades de control se implementan, entre otros, mediante políticas y procedimientos que deben ser revisados cuando ocurren cambios significativos para mantener su eficiencia operacional.

La Junta de Gobierno de la Administración es responsable de aprobar los reglamentos y velar por su implementación; y el administrador debe velar por el cumplimiento de los reglamentos aprobados y aquellos integrados por la Administración. En los aspectos relacionados con la formulación de la política pública que regirá los sistemas de información computadorizados, la administradora auxiliar del ASIT asesora y ofrece apoyo al administrador.

El examen realizado de las políticas, normas y procedimientos relacionados con las operaciones de los sistemas de información computadorizados de la Administración reveló que al 14 de agosto de 2024 no contaba con políticas, normas y procedimientos aprobados necesarios para controlar las siguientes operaciones:

- Administrar y controlar los accesos lógicos y físicos a los recursos de tecnología de información.
- Administrar la red. Las normas presentadas para examen no estaban aprobadas, eran generales, no establecían el personal responsable.
- Administrar la seguridad de los sistemas de información computadorizados.
- Administrar la ciberseguridad y, detectar, reportar y responder a incidentes de seguridad.
- Preparar, almacenar y controlar los respaldos. En su lugar mantenía el *AVP Backup and Restore Guide* que no estaba aprobado y no incluía procedimientos específicos aplicables a la Administración.
- Controlar las actualizaciones de las aplicaciones.
- Controlar el uso de los sistemas de información computadorizados. En su lugar mantenía, el documento *Advertencias electrónicas-avp Internet* que no estaba aprobado, un memorando dirigido a los usuarios de los sistemas de información que incluía unas normas generales en cuanto al uso de las computadoras y otro memorando sobre el uso del correo electrónico que se basaba en una reglamentación de la Oficina de Gerencia y Presupuesto que esta derogada.
- Decomisar y donar equipo computadorizado.
- Promover las mejores prácticas en relación con la clasificación y publicación de los datos en cumplimiento con la *Ley 40-2024*.

Criterios

Las situaciones comentadas son contrarias a las siguientes disposiciones:

- Artículos 7. (g) y (h) de la *Ley 151-2004*
- Principios 10.02, 11.01, 12.01, 12.02 y 12.05 de la Sección Actividades de Control del *Green Book*

Efectos

Las situaciones comentadas tienen los siguientes efectos:

- Impide a la Administración mantener un control eficaz sobre las operaciones relacionadas con sus sistemas de información computadorizados.
- Impide adjudicar responsabilidades en los casos de que se cometan irregularidades utilizando sus sistemas de información computadorizados.

Causas

Las situaciones identificadas responden, entre otras cosas, por lo siguiente:

- La administradora auxiliar del ASIT nos certificó que los documentos suministrados son borradores y no están acorde con las nuevas tecnologías. Además, que se le ha dificultado completar la actualización de estos debido a la falta de recursos en la ASIT.

Recomendaciones 1 y 3.a.

Recomendaciones

Al secretario del Departamento de la Vivienda

1. Ver que el administrador cumpla con las **Recomendación 3** para que se corrijan y no se repitan las situaciones comentadas en los **hallazgos del 1 al 6**.
2. Impartir instrucciones a la secretaria auxiliar de Recursos Humanos del Departamento para que en coordinación con la administradora auxiliar del ASIT cumpla con la **Recomendación 3.g.** de este *Informe*. **[Hallazgo 2-a.]**

Al Administrador

3. Ejercer una supervisión efectiva para asegurarse de que la administradora auxiliar del ASIT:
   a. Identifique los recursos necesarios y prepare las políticas administrativas y operacionales o procedimientos relacionados con las operaciones críticas de los sistemas de información computadorizados. Una vez se aprueben estas políticas por la gerencia deberán ser revisados cada vez que surja un cambio significativo dentro de la infraestructura tecnológica de la Administración, para asegurarse que dichos planes se mantengan actualizados. **[Hallazgos 1-a. y 6]**
   b. Actualice el diseño del formulario de acceso al Sistema Yardi y lo remita para su aprobación como parte del procedimiento para otorgar el acceso lógico a los sistemas de información. **[Recomendación 3.a.]** Además, que luego de aprobado el procedimiento se actualicen los formularios de acceso de los usuarios activos y se asegure que se informe al personal sobre la importancia de que este sea utilizado y completado con toda la información requerida para identificar apropiadamente al usuario y los privilegios autorizados. **[Hallazgo 1-a.]**
   c. Documente todas las cuentas de acceso al Sistema Yardi con privilegios administrativos. Además, evalúe y determine la pertinencia de estas cuentas de acceso para otorgar el mismo solo al personal que lo necesite para realizar sus tareas y funciones específicas, y esté autorizado a tener estos privilegios en el sistema. **[Hallazgo 1-b.]**
   d. Desactive inmediatamente las cuentas de acceso asignadas a los exempleados cuando le sea notificado a la ASIT por la Secretaría Auxiliar de Recursos Humanos del Departamento. **[Hallazgo 2-a.]**
   e. Evalúe la necesidad de las 483 cuentas de acceso activas mencionadas en el **Hallazgo 2-b.** y desactive las que no son necesarias.
   f. Realice las gestiones necesarias con la compañía de consultoría para corregir el problema del envío del informe de las cuentas que no han tenido activad dentro de los últimos 90 días. Una vez este informe sea corregido, mantener una revisión oportuna de los accesos realizados y cuentas inactivas, e inactivar aquellas cuentas no utilizadas que cumplan con los criterios establecidos por la Administración. **[Hallazgo 2-b.]**
   g. En coordinación con la secretaria auxiliar de Recursos Humanos del Departamento, prepare un procedimiento para el trámite de renuncias, traslados o cesantías de empleados usuarios de los sistemas de información de la administración, que requiera, entre otras cosas, la notificación oportuna de las renuncias, traslados o cesantías a la ASIT y lo refiera para aprobación del administrador. Una vez aprobado, deberá mantenerse actualizado para que incluya cualquier cambio significativo dentro de la estructura organizacional del Departamento y de la Administración. **[Hallazgo 2-b.]**
   h. Identifique alternativas costo-efectivas para preparar, documentar y remitir para aprobación un análisis de riesgo que considere todos los sistemas de información computadorizados de la Administración. Además, una vez aprobado, ver que se revise cada vez que surja un cambio significativo dentro de la infraestructura operacional y tecnológica de la Administración, para asegurarse de que se mantenga actualizado. **[Hallazgo 3]**
   i. Realice las gestiones necesarias para preparar y remitir para la aprobación del administrador un programa de ciberseguridad conforme con lo establecido en la *Ley 40-2024* y un procedimiento para el manejo de incidentes. Entre estas, considere asignar personal adicional al ASIT que cuente con conocimiento sobre los elementos básicos de un programa de ciberseguridad y el manejo de incidentes de seguridad. **[Hallazgo 4]**

j. Prepare y remita para la aprobación del administrador el plan de contingencia y el plan para la recuperación de desastres relacionados con sus sistemas de información computadorizados. Una vez aprobados, deberán ser revisados cada vez que surja un cambio significativo dentro de la infraestructura tecnológica de la Administración, para asegurarse que los mismos se mantengan actualizados. Además, debe realizar anualmente, al menos, un ejercicio o una prueba simulando escenarios de desastre o interrupción de servicio para, entre otras cosas, evaluar la efectividad de los procedimientos establecidos. **[Hallazgo 5]**

Información sobre la unidad auditada

La Administración se creó mediante la *Ley 66-1989*, según enmendada. Esta es responsable de mejorar la calidad de vida de los residenciales públicos, y fomentar la actividad comunitaria y el desarrollo personal y familiar de los residentes. La Administración está adscrita al Departamento, y esta tiene la finalidad y la función de lograr una administración de los residenciales públicos altamente eficiente y con la flexibilidad necesaria para la ejecución de la política pública de mejorar la calidad de vida en los residenciales públicos, fomentar la actividad comunitaria y el desarrollo integral de los puertorriqueños que viven en dichos proyectos de vivienda.

Los poderes, funciones y responsabilidades de la Administración son ejercidos por la Junta de Gobierno de la Administración de Vivienda Pública (Junta), la cual está integrada por siete miembros: el secretario de Vivienda, quien es el presidente; el secretario del Departamento de la Familia, el secretario del Departamento del Trabajo y Recursos Humanos, el director ejecutivo de la Autoridad para el Financiamiento de la Vivienda, quienes son miembros exoficio de la Junta; y tres representantes del sector privado nominados por el secretario de la vivienda con la aprobación del gobernador. De los representantes del sector privado, dos deben ser seleccionados entre los residentes de dos residenciales públicos distintos y un representante del sector privado[8]. Los miembros del sector privado sirven tres años cada uno.

El administrador es nombrado por el gobernador, con el consejo y consentimiento del Senado del Estado Libre Asociado de Puerto Rico. El administrador desempeña el cargo a voluntad de la Junta y debe ser una persona de amplia preparación y experiencia profesional en las áreas de gerencia y administración pública, haber demostrado un genuino interés en el estudio y la aplicación de las ciencias sociales y estar comprometido con la consecución de los objetivos de la ley de la Administración.

La Administración se compone de las oficinas del Administrador; de Proyectos Especiales; de Asesoramiento Legal; de Seguridad; de Cumplimiento - Sección 504; y de Reglamentación y Cumplimiento. Además, se compone de las áreas de Finanzas y Administración; Programas Comunales y de Residentes; Adquisiciones y Contrataciones; Desarrollo y Construcción de Proyectos; Administración de Proyectos; Selección y Ocupación; y Sistemas de Información Tecnológica y del Programa de Vales para la Libre Selección de Vivienda (Sección 8). También presta sus servicios mediante 10 oficinas regionales[9] del Área de Selección y Ocupación y 9 oficinas regionales[10] del Programa de Vales para la Libre Selección de Vivienda (Sección 8).

El Programa de Vivienda Pública, que surge de la Sección 9 de la *Ley Federal de 1937*, se estableció para brindar viviendas públicas seguras en alquiler para familias e individuos de bajos ingresos, ancianos y personas incapacitadas que reúnan los requisitos necesarios. Existen viviendas públicas de todo tipo y tamaño, desde viviendas unifamiliares dispersas hasta

[8] Este debe tener preparación o experiencia profesional, sin que se entienda como una limitación, en una o más de las siguientes áreas: trabajo social, psicología, salud mental, sociología, planificación familiar, contabilidad, gerencia o administración pública, administración de empresas, educación física, urbanismo o planificación.

[9] Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Humacao, Guayama, Mayagüez, Ponce y San Juan.

[10] Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Humacao, Mayagüez, Ponce y San Juan.

apartamentos en torre para familias de ancianos. La Administración establece las normas de ocupación para asegurarse que las unidades serán ocupadas según la composición familiar. Esto asegura una máxima ocupación de las unidades al mismo tiempo evita el uso indebido, hacinamiento, desgaste, vandalismo o falta de aprovechamiento de estas.

El presupuesto asignado a la Administración proviene de Fondos Especiales Estatales, Fondos Federales, Ingresos Propios, Resolución Conjunta del Presupuesto General, Asignaciones Especiales y Otros Ingresos. El presupuesto asignado a la Administración durante los años fiscales 2021-22 al 2023-24, ascendió a $562,104,000, $899,970,000, y $652,670,000, respectivamente.

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

La Administración cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.avp.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 Sr. Juan A. Rosario Hernández, administrador, mediante cartas de nuestros auditores del 27 de mayo y del 18 de junio de 2025. En la segunda carta se incluyeron anejos con detalles sobre las situaciones comentadas.

El administrador remitió sus comentarios mediante cartas del 12 de junio y del 7 de julio de 2025 los cuales se consideraron al redactar el borrador de este *Informe*.

Mediante correos electrónicos del 30 de octubre de 2025 remitimos, para comentarios, lo siguiente:

- El borrador de este *Informe* a la Sra. Ciary Y. Pérez Peña, exsecretaria de la Vivienda, y al Sr. Juan A. Rosario Hernández, administrador.
- El borrador de los hallazgos al Lcdo. William O. Rodríguez Rodríguez, exsecretario de la Vivienda, y al Lcdo. Alejandro E. Salgado Colón, exadministrador.

El director ejecutivo remitió sus comentarios mediante carta enviada por correo electrónico del 24 de noviembre de 2025, los cuales se consideraron al redactar el borrador de este *Informe*. Además, entre otras cosas, relacionado con los **hallazgos 3 al 6** de este *Informe* nos indicó lo siguiente:

> […] El análisis que realizó la administradora auxiliar del área de sistemas de información me informó que la agencia no estaría cumpliendo con varios requisitos mencionados. Esto se debe a que la Administración no cuenta con el personal especializado para realizar este tipo de análisis, por lo cual solicité que se realizara el proceso de contratación para atender lo antes mencionado. Una vez nos llegue la aprobación de la contratación, el área de sistemas de información puede comenzar los procesos en conjunto con la compañía contratada. [*sic*]

La exsecretaria, el exsecretario y el ex director ejecutivo no remitieron sus comentarios.

Control interno

La gerencia de la Administración 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 de la Administración.

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. Además, en los **hallazgos 3 al 6** se comentan deficiencias de controles internos relacionadas con la administración de la seguridad y la continuidad del servicio, 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 1 de enero de 2022 al 4 de junio de 2025. El examen lo efectuamos de acuerdo con las normas de auditoría generalmente aceptadas contenidas en el *Goverment Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos (GAO por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de 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; exámenes de expedientes, pruebas y análisis de procedimientos de control interno y de otros procesos.

Para realizar esta auditoría utilizamos las leyes *151-2004* y *40-2024,* las políticas *TI-PRITS-004*, *TI-PRITS-005* y *TI-PRITS-007* y la *Política para la Seguridad Cibernética*, entre otros. Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica; el capítulo 3 del *FISCAM*, y la sección Actividades de Control del *Green Book*, emitidos por el GAO. Aunque a la Administración no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información y la administración.

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

Además, como parte de nuestro segundo objetivo de auditoría evaluamos la confiabilidad de los datos obtenidos del Sistema Yardi, que contiene, entre otros, la información de los solicitantes, de las listas de espera, los participantes del programa de vivienda pública y los pagos recibidos por concepto de renta desde el 1 de enero de 2022 al 31 de diciembre de 2024. Como parte de dicha evaluación, entrevistamos a los funcionarios con conocimiento del sistema y de los datos; realizamos pruebas electrónicas para detectar errores de precisión e integridad, y revisamos la documentación e información existente sobre los datos y el sistema que los produjo. Determinamos que los datos son suficientemente confiables para los objetivos de este *Informe*.

Anejo 1 - Funcionarios principales de la Junta de Gobierno durante el período auditado

NOMBRE	PUESTO	PERÍODO	
		DESDE	HASTA
Sra. Ciary Y. Pérez Peña	Presidenta	2 ene. 25	13 jun. 25
Lcdo. William O. Rodríguez Rodríguez	Presidente	1 ene. 22	31 dic. 24

Anejo 2 – Funcionarios principales de la entidad durante el período auditado

NOMBRE	PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Juan A. Rosario Hernández	Administrador[11]	24 feb. 25	13 jun. 25
Lcdo. Alejandro E. Salgado Colón	”	1 ene. 22	13 sep. 24
Sr. Alberto E. Fradera Vázquez	Subadministrador[12]	10 mar. 25	13 jun. 25
Lcda. Irmaris Vicenty Berríos	Subadministradora	1 ene. 22	10 feb. 25
Sra. Lymari De Jesús Fuentes	Administradora auxiliar del Área de Sistemas de Información Tecnológicas	1 ene. 22	13 jun. 25
Sra. Odaly Román Díaz	Administradora asociada del Área de Selección y Ocupación de Residentes	18 jul. 22	13 jun. 25
Lcdo. Omar Figueroa Vázquez	Administrador asociado del Área de Selección y Ocupación de Residentes	1 ene. 22	15 jul. 22
Lcda. Lisneida Nieves Martínez	Secretaria auxiliar de Recursos Humanos	1 ene. 23	13 jun. 25

[11] El puesto estuvo vacante del 14 de septiembre de 2024 al 23 de febrero de 2025.

[12] El puesto estuvo vacante del 11 de febrero al 9 de marzo de 2025.

Fuentes legales

Estatutos federales

United States Housing Act of 1937, 42 U.S.C. § 1437 et seq. (*Ley Federal de 1937*). (1937).

Leyes

Ley 40-2024. *Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico.* (*Ley 40-2024*). 18 de enero de 2024.

Ley 66 de 1989. *Ley Orgánica de la Administración de Vivienda Pública de Puerto Rico*. (*Ley 66-1989*). 17 de agosto de 1989.

Ley 151 de 2004. *Ley de Gobierno Electrónico*. (*Ley 151-2004*). 22 de junio de 2004.

Reglamentación (reglamentos, normas, manuales, procedimientos)

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

GAO-14-704G. (2014). [Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos]. Standards For Internal Control in the Federal Government (*Green Book*). Septiembre de 2014.

Reglamento 8624 de 2015. [Administración de Vivienda Pública]. *Reglamento sobre las Políticas de Admisión y Ocupación Continuada en los Residenciales Públicos del Estado Libre Asociado de Puerto Rico*. 31 de julio de 2015.

Cartas circulares

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

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

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 2024.

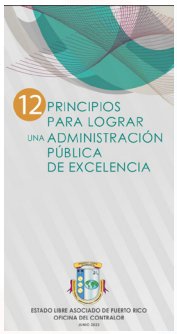
Política TI-PRITS-005. [Puerto Rico Innovation and Technology Service]. *Política sobre las Mejores Prácticas de Infraestructura Tecnológica.* 30 de junio de 2023.

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

OFICINA de la CONTRALORA
GOBIERNO DE PUERTO RICO

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 postal, teléfono o mediante correo electrónico. Puede obtener más información en la página de Internet de la Oficina, sección *Queréllese*.