

INFORME DE AUDITORÍA TI-21-14

8 de junio de 2021

Departamento de Justicia

Oficina de Informática

(Unidad 5270 - Auditoría 14367)

Período auditado: 10 de octubre de 2019 al 25 de septiembre de 2020

CONTENIDO

	Página
OBJETIVOS DE AUDITORÍA.....	2
CONTENIDO DEL INFORME.....	3
ALCANCE Y METODOLOGÍA.....	3
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	4
COMUNICACIÓN CON LA GERENCIA.....	7
CONTROL INTERNO.....	8
OPINIÓN Y HALLAZGOS.....	8
1 - Deficiencias relacionadas con el Plan de Respuesta de Emergencias y Recuperación	9
2 - Falta de desactivación de cuentas de acceso a la red de comunicación del Departamento	10
RECOMENDACIONES.....	13
APROBACIÓN	13
ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO.....	14

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

8 de junio de 2021

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

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

**OBJETIVOS DE
AUDITORÍA**

Objetivo general

Determinar si las operaciones de la Oficina de Informática del Departamento se efectuaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

1. Determinar si el *Plan de Riesgo de la Oficina de Informática* contiene los requisitos necesarios establecidos en la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el entonces director de la Oficina de Gerencia y Presupuesto.

2. Determinar si las cuentas de acceso de exempleados o exusuarios externos fueron desactivadas conforme a lo requerido en el *Manual de las Normas, Procedimientos y Políticas de Seguridad (Manual)* aprobado el 10 de octubre de 2019¹ por la secretaria de Justicia.
3. Determinar si el *Plan de Respuesta de Emergencias y Recuperación* está de acuerdo con la infraestructura tecnológica del Departamento y sus operaciones, y si contienen los requisitos que son necesarios para atender situaciones de emergencia.

CONTENIDO DEL INFORME

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 10 de octubre de 2019 al 25 de septiembre de 2020. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo que concierne a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como: entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

¹ La versión anterior del *Manual* fue aprobada el 20 de abril de 2010 y contenía disposiciones similares.

Al realizar esta auditoría utilizamos el *Manual* y las políticas establecidas en la *Carta Circular 140-16*. Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica las guías establecidas en el *Federal Information Systems Controls Audit Manual (FISCAM)*², emitido por el GAO. Aunque al Departamento no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento se creó en virtud de la Sección 6 del Artículo IV de la Constitución del Estado Libre Asociado de Puerto Rico. El 9 de agosto de 2004; mediante la *Ley 205-2004, Ley Orgánica del Departamento de Justicia*, según enmendada, se establecieron, entre otras cosas, las funciones y los deberes del secretario de Justicia, así como la organización interna del Departamento.

El *Plan de Reorganización Núm. 5 del 27 de diciembre de 2011, Plan de Reorganización del Departamento de Justicia 2011*³, reorganizó el Departamento, a través de la delegación de sus poderes y responsabilidades en nuevas secretarías auxiliares, la eliminación de estructuras paralelas y la descentralización del poder decisonal, delegado en los fiscales de distrito para lograr obtener un procesamiento criminal más efectivo.

Las funciones principales del Departamento son ofrecer asesoramiento legal al gobernador, a la Asamblea Legislativa, a los jefes de agencias y a los alcaldes; proveer representación legal a las instituciones del Gobierno de Puerto Rico y a sus funcionarios o empleados; e investigar y procesar

² El *FISCAM* utiliza las guías emitidas por el National Institute of Standard and Technology.

³ El 10 de abril de 2017 se aprobó la *Ley 20-2017, Ley del Departamento de Seguridad Pública de Puerto Rico*, la cual derogó el Capítulo III del *Plan de Reorganización Núm. 5* y se consolidaron en el Departamento de Seguridad Pública los servicios que brindaba el Negociado de Investigaciones Especiales.

ante los tribunales a los imputados de delito, las querellas contra menores de edad que han cometido faltas, así como los casos de maltrato de menores; representar los intereses de los menores en los procedimientos judiciales sobre protección de los menores y atender asuntos civiles relacionados con la institución familiar; implantar las leyes antimonopolios; mantener un sistema mecanizado de procesamiento de información sobre Justicia Criminal; y proveer certeza con relación al tráfico jurídico de bienes inmuebles mediante el Registro de la Propiedad.

Conforme a lo dispuesto en la Constitución, el Departamento está adscrito a la Rama Ejecutiva del Gobierno. El mismo es dirigido por un secretario de Justicia nombrado por el gobernador con el consejo y consentimiento del Senado de Puerto Rico.

El Departamento está compuesto por las oficinas del Secretario y del Subsecretario, Informática, Ayuda al Ciudadano, Jefes de los Fiscales, y Procurador General. Además, cuentan con las divisiones de Seguridad e Integridad Pública y Asuntos del Contralor, la Biblioteca Legal y las secretarías auxiliares de Gerencia y Administración, Recursos Humanos, Asuntos de Menores y Familia, Asuntos Monopolísticos, de lo Civil, y Asesoramiento. También están adscritas al Departamento la Junta de Confiscaciones, el Sistema de Información de Justicia Criminal, la Unidad de Control de Fraude al Medicaid, el Instituto de Capacitación y Desarrollo del Pensamiento Jurídico, la Oficina de Compensación y Servicios a las Víctimas y Testigos de Delitos, y la Oficina Administrativa del Registro Inmobiliario Digital.

El Departamento presta servicios a través de 13 fiscalías localizadas en Aguadilla, Aibonito, Arecibo, Bayamón, Caguas, Carolina, Fajardo, Guayama, Humacao, Mayagüez, Ponce, San Juan, y Utuado. Estas son dirigidas por fiscales de distrito que le responden a la Oficina del Jefe de los Fiscales.

Mediante la *Orden Administrativa 2017-11* del 27 de diciembre de 2017, se estableció la figura del principal asesor en tecnología del Departamento.

El principal asesor en tecnología es responsable de los sistemas de tecnología de información de la agencia a nivel de procesos electrónicos y de la planificación necesaria para la adquisición de nuevos equipos y programas.

Mediante la *Orden Administrativa 2020-02*⁴ del 6 de agosto de 2020, se denominó al principal asesor en tecnología del Departamento como principal oficial en tecnología e informática del Departamento. Este es responsable de fiscalizar y monitorear los avances tecnológicos y proyectos de innovación del Departamento y sus organismos adscritos. Además, dirige, evalúa, ejecuta y supervisa la administración de los recursos en el área de tecnología del Departamento y sus componentes adscritos. También funge como enlace del Departamento con el Puerto Rico Innovation and Technology Service (PRITS) y establece con ese organismo, una coordinación efectiva que permita maximizar los recursos tecnológicos del Gobierno.

La Oficina de Informática cuenta con 18 puestos autorizados, de los cuales 9 están ocupados: 1 director de sistemas de informática, 2 gerentes de sistemas de informática, 2 desarrolladores de sistemas de informática, y 4 técnicos de sistemas de informática. Los puestos vacantes son: 2 gerente de sistemas de informática, 1 desarrollador de sistemas de informática, y 6 técnicos de sistemas de informática.

A la fecha de nuestra auditoría, el Departamento tenía una red local de área (LAN, por sus siglas en inglés) que interconectaba 1,411 usuarios mediante tecnología de fibra óptica, cables y conexión inalámbrica. Además, mantenían en producción 10 sistemas adquiridos y 14 desarrollados, y utilizaba el Sistema de Recursos Humanos Mecanizados (RHUM), el Puerto Rico Integrated Financial Accounting System (PRIFAS) y el Sistema de Ingresos y Recaudos - Área de Tesorero (SIRAT) para procesar las nóminas, registrar las operaciones financieras, manejar y controlar las recaudaciones.

⁴ Esta deroga la *Orden Administrativa 2017-11*.

Los recursos para financiar las operaciones del Departamento provienen de asignaciones especiales, fondos especiales estatales, fondos federales, otros ingresos y la resolución conjunta del presupuesto general. El presupuesto aprobado para los años fiscales del 2018-19 al 2020-21, ascendió a \$158,443,000, \$143,044,000, y \$136,837,000, respectivamente. La Oficina de Informática no cuenta con un presupuesto propio. Sus gastos son sufragados por el Programa de Dirección y Administración General.

El **ANEJO** 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: www.justicia.pr.gov. Esta página provee información acerca del Departamento y de los servicios que ofrece.

COMUNICACIÓN CON LA GERENCIA

El 5 de marzo de 2021 remitimos el borrador de este *Informe* para comentarios del Hon. Domingo Emanuelli Hernández, secretario de Justicia; y el borrador de los **hallazgos** para comentarios de la Lcda. Dennise N. Longo Quiñones, exsecretaria, y de la Lcda. Inés del C. Carrau Martínez, ex secretaria interina.

El 15 de marzo de 2021 la licenciada Longo Quiñones contestó y nos indicó, entre otras cosas, que concurría plenamente con la intención de la auditoría y con el objetivo de lograr que la Oficina de Informática del Departamento logre cumplir cabalmente con los procesos y requisitos establecidos en los protocolos y reglamentos de la agencia, con respecto a las cuentas de informática. Además, que es importante que el Departamento establezca, mantenga e implemente oportunamente controles de acceso para la utilización de su información (muchas de la cual es confidencial y relacionada con investigaciones sensitivas de ley y orden). También indicó que durante su tiempo como secretaria trabajó de la mano con el personal de la Oficina de Informática y la Secretaría Auxiliar de Gerencia y Administración para alcanzar el cumplimiento requerido.

Mediante carta del 23 de marzo de 2021 el secretario de Justicia contestó el borrador de este *Informe*. En los **hallazgos** se incluyeron algunos de sus comentarios.

La licenciada Carrau Martínez no contestó.

CONTROL INTERNO

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

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

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

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

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

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la Oficina de Informática del Departamento objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con

las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos 1 y 2** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con el Plan de Respuesta de Emergencias y Recuperación

Situación

- a. Toda entidad gubernamental debe contar con un plan de contingencias, para reestablecer sus operaciones más importantes en caso de que surja una emergencia. El mismo debe incluir toda la información y los procesos necesarios para recuperar las operaciones de los sistemas de información computadorizados.

El Departamento cuenta con el *Plan de Respuesta de Emergencias y Recuperación* aprobado el 20 de marzo de 2019 por el entonces principal asesor en tecnología y por la entonces directora de sistemas de informática.

El 9 de marzo de 2020 realizamos un examen de dicho *Plan*. Este reveló que no se incluyó la siguiente información, necesaria para atender situaciones de emergencias:

- 1) Los sistemas operativos y los archivos críticos de la Oficina de Informática
- 2) Los proveedores primarios, incluido el número de teléfono y nombre del personal de enlace con la entidad
- 3) El procedimiento para efectuar pruebas en el centro alerno.

Criterio

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

Efecto

La situación comentada podría propiciar la improvisación y que, 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 de los servicios a los usuarios del Departamento.

Causas

La entonces directora de Sistemas de Informática entendía que no era importante incluir la información de los proveedores primarios en el *Plan*, porque era un proveedor privado y cambiaba constantemente la persona contacto, y que el inventario de los sistemas operativos y los archivos críticos estaban incluido en el *Plan de Riesgo* de la Oficina de Informática. Además, no incluyó un procedimiento para efectuar pruebas al centro alerno porque era una tarea diaria de monitoreo en la Oficina Informática.

Comentarios de la Gerencia

El secretario de Justicia nos indicó, entre otras cosas, lo siguiente:

Se impartieron instrucciones al director de la oficina de tecnología e informática para que revise y remita para mi aprobación el Plan de Respuesta de Emergencia y Recuperación que incluya los sistemas operativos y los archivos críticos de la Oficina de Informática, los proveedores primarios con su número de teléfono y nombre del personal de enlace con la entidad. [sic]

Véase la Recomendación 1.a.**Hallazgo 2 - Falta de desactivación de cuentas de acceso a la red de comunicación del Departamento****Situación**

- a. Las entidades gubernamentales deben implementar controles de acceso para la utilización de la información y los programas de aplicación, de forma que estos sean accedidos solo por el personal autorizado. Las cuentas de acceso a los sistemas de información deben administrarse para controlarlas eficazmente e identificar y autenticar a los usuarios. También se deben revisar periódicamente las listas de autorizaciones de las cuentas de accesos a los sistemas de información para determinar si son apropiadas. Además, la entidad

debe asegurarse de que los administradores de las cuentas reciban una notificación cuando los usuarios de los sistemas de información cesan funciones o se transfieren para que se eliminen, inactiven o aseguren las cuentas de acceso asignadas.

En el Anejo C, Procedimiento para eliminar la Cuenta del Usuario del *Manual*, se requiere cumplimentar el Inciso I de la *Certificación de Devolución de la Propiedad (Certificación)*, a todo empleado que tenga conocimiento oficial de su salida del Departamento, con antelación a su último día de trabajo. Posteriormente, se debe continuar con el proceso de cancelar los accesos correspondientes a los sistemas del Departamento. La cuenta del empleado debe quedar activa durante 30 días, para que su supervisor inmediato tenga acceso a alguna información relacionada con las tareas que este ejercía.

Además, el secretario auxiliar de Recursos Humanos debe informar a la Oficina de Informática cuando un empleado cese en sus funciones. El gerente de sistemas de informática es el responsable de desactivar las cuentas una vez transcurridos los 30 días posteriores a la fecha del cese de funciones de los empleados.

Al 11 de octubre de 2019, el Departamento tenía 1,396 cuentas de usuarios activas.

El examen realizado sobre el mantenimiento de 134 cuentas de acceso a la red de comunicación del Departamento, reveló que, al 6 de julio de 2020, no se habían desactivado 57 cuentas de acceso que correspondían a 48 exempleados, 5 excontratistas y 4 personas que estuvieron por destaque en el Departamento y que cesaron en sus funciones entre el 31 de diciembre de 2010 y el 31 de enero de 2020. A la fecha del examen, habían transcurrido entre 157 y 3,475 días desde la separación de estos. De estas cuentas 28 fueron utilizadas, entre 31 y 2,215 días, luego de las fechas de separación.

Criterios

La situación comentada es contraria a lo establecido en la Sección E.6. de la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*; en el Capítulo 3.2, Access Control, del *FISCAM*; y en el Anejo C, Procedimiento para eliminar la Cuenta del Usuario, del *Manual*.

Efectos

Las situaciones comentadas pueden propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados de la red de comunicaciones del Departamento sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

La situación comentada se debió a que el secretario auxiliar de Recursos Humanos no informaba a la Oficina de Informática cuando un empleado cesaba funciones. Además, la Oficina de Informática no recibía las certificaciones de devolución de la propiedad para cancelar las cuentas de accesos o los recibía luego de un tiempo prolongado. Tampoco se le requería completar dicha *Certificación* a los contratistas y al personal que estaba por destaque en el Departamento.

Comentarios de la Gerencia

El secretario de Justicia nos indicó, entre otras cosas, lo siguiente:

[...] la Oficina de Informática está trabajando un proceso de coordinación para que la SARH y toda oficina que contrate personal, notifique la cancelación de cuentas de empleados, destakes y contratistas que cesen sus funciones en el Departamento. [sic]

Se impartieron instrucciones a la Oficina de Informática para que [...] se cumplan con las directrices establecidas en el Procedimiento para eliminar la Cuenta del Usuario del Manual sobre la desactivación de las cuentas de usuario una vez cesen en sus funciones. [sic]

Véanse las recomendaciones 1.b. y 2.

RECOMENDACIONES**Al secretario de Justicia**

1. Ver que el principal oficial en tecnología e informática se asegure de que el director de sistemas de informática cumpla con lo siguiente:
 - a. Revise el *Plan* y lo remita para su aprobación, y se asegure de que la información contenida en este se actualice para incluir los aspectos comentados en el **Hallazgo 1**.
 - b. Imparta instrucciones al gerente de sistemas de informática para que desactive las cuentas de acceso comentadas en el **Hallazgo 2**, y vea que, en lo sucesivo, se desactiven en el momento en que el usuario cese en sus funciones y se cumpla con las directrices establecidas en el Procedimiento para eliminar la Cuenta del Usuario del *Manual*.
2. Asegurarse de que los secretarios auxiliares de Recursos Humanos y Asesoramiento, en coordinación con el principal oficial en tecnología e informática, establezcan un procedimiento para notificar a tiempo a la Oficina de Informática el cese de un usuario en sus funciones, para la desactivación de la cuenta de acceso de este. [**Hallazgo 2**]

APROBACIÓN

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.

Oficina del Contralor de Puerto Rico

Aprobado por:



ANEJO

DEPARTAMENTO DE JUSTICIA
OFICINA DE INFORMÁTICA
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcda. Inés del C. Carrau Martínez	Secretaria Interina de Justicia	8 jul. 20	25 sep. 20
Lcda. Dennise N. Longo Quiñones	Secretaria de Justicia	10 oct. 19	3 jul. 20
Lcdo. Víctor M. Carbonell Ramírez	Subsecretario Interino de Justicia	24 ago. 20	25 sep. 20
Lcda. Tanya García Ibarra	Subsecretaria de Justicia ⁵	27 feb. 20	30 jun. 20
Lcda. Grisel Santiago Calderón	"	10 oct. 19	4 feb. 20
Lcdo. Christian A. Castro Plaza	Secretario Auxiliar de Recursos Humanos ⁶	15 ene. 20	25 sep. 20
Lcdo. Daniel Vélez Cabrera	Secretario Auxiliar de Asesoramiento ⁷	29 may. 20	25 sep. 20
Lcda. Mairís A. Cassagnol Cornier	Secretaria Auxiliar de Asesoramiento	10 oct. 19	30 abr. 20
Sr. Luis C. Capre Martínez	Principal Oficial en Tecnología e Informática	4 jun. 20	25 sep. 20
Lcdo. Néstor L. Márquez Rivera	Principal Asesor en Tecnología ⁸	10 oct. 19	30 abr. 20
Sr. José Sánchez Medina	Director de Sistemas de Informática ⁹	29 may. 20	25 sep. 20
Sra. Enid Soto Ortiz	Directora de Sistemas de Informática	10 oct. 19	18 feb. 20

⁵ Del 6 al 26 de febrero de 2020, la licenciada García Ibarra ocupó el puesto interinamente. Este puesto estuvo vacante del 1 de julio al 23 de agosto de 2020.

⁶ Del 10 de octubre de 2019 al 14 de enero de 2020, el licenciado Castro Plaza ocupó el puesto interinamente.

⁷ Este puesto estuvo vacante del 1 al 28 de mayo de 2020.

⁸ Este puesto se denominó principal oficial en tecnología e informática mediante la *Orden Administrativa 2020-02* y estuvo vacante del 1 de mayo al 3 de junio de 2020.

⁹ Este puesto estuvo vacante del 19 de febrero al 28 de mayo de 2020.

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069