

Brunilda Ortiz Rodríguez
30/Nov/2012



Secretaria

Brunilda Ortiz Rodríguez

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- Expediente
- Dar Cuenta
- Registrar y Procesar

Senado
DE PUERTO RICO

EL CAPITOLIO
PO Box 9023431
San Juan, Puerto Rico
00902-3431

T: 787.722.3460

787.722.4012

F: 787.723.5413

W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

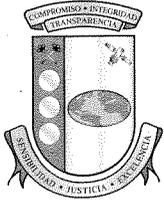
- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico y Planificación
- Urbanismo e Infraestructura
- Jurídico Penal
- Jurídico Civil
- Agricultura
- Recursos Naturales y Ambientales
- Comercio y Cooperativismo
- Turismo y Cultura
- Trabajo, Asuntos del Veterano y Recursos Humanos
- Bienestar Social
- Asuntos Municipales
- Recreación y Deportes
- Banca, Asuntos del Consumidor y Corporaciones Públicas
- Desarrollo de la Región del Oeste
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario
- Asuntos Federales
- De la Montaña
- Ética

COMISIONES ESPECIALES

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

COMISIONES CONJUNTAS

- Informes Especiales del Contralor
- Donativos Legislativos de Puerto Rico
- Internado Córdova-Fernós
- Internado Pilar Barbosa
- Internado Ramos Comas
- Código Penal
- Revisión y Reforma del Código Civil
- Alianzas Público Privadas
- Auditoría Fiscal y Manejo Fondos Públicos
- Revisión Continua Código Penal y Reforma de las Leves



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

29 de noviembre de 2012

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copias de los informes de auditoría *TI-13-09* y *TI-13-10* de la Oficina de Tecnología Cibernética del Departamento de Estado y del Departamento de Informática de la Oficina del Procurador del Ciudadano, respectivamente, aprobados por esta Oficina el 27 de noviembre de 2012. Publicaremos dichos informes en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,


Yesmín M. Valdivieso

Anejos

RECIBIDO
OFICINA PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ
2012 NOV 29 PM 3:10

INFORME DE AUDITORÍA TI-13-09

27 de noviembre de 2012

Departamento de Estado

Oficina de Tecnología Cibernética

(Unidad 5265 - Auditoría 13576)

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ
2012 NOV 29 PM 3:10

Período auditado: 8 de octubre de 2010 al 14 de abril de 2011

CONTENIDO

	Página
ALCANCE Y METODOLOGÍA	2
CONTENIDO DEL INFORME	2
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	3
COMUNICACIÓN CON LA GERENCIA	5
OPINIÓN Y HALLAZGOS	6
1 - Falta de un plan de seguridad, y de adiestramientos relacionados con la seguridad de los sistemas de información computadorizados	6
2 - Falta de un plan de continuidad de negocios, de pruebas o simulacros para probar la efectividad del Plan de Contingencia, y de acuerdos para mantener un centro alternativo de recuperación de sistemas de información.....	9
RECOMENDACIONES	12
AGRADECIMIENTO	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

27 de noviembre de 2012

Al Gobernador, al Presidente del Senado
y a la Presidenta de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la Oficina de Tecnología Cibernética (OTC) del Departamento de Estado (Departamento) para determinar si se efectuaron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. 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.

**ALCANCE Y
METODOLOGÍA**

La auditoría cubrió del 8 de octubre de 2010 al 14 de abril de 2011. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

**CONTENIDO DEL
INFORME**

Este es el primer informe y contiene dos hallazgos sobre el resultado del examen de los controles internos establecidos para la administración del programa de seguridad, el acceso lógico a los sistemas de información computadorizados, la continuidad del servicio y la red de comunicaciones del Departamento.

**INFORMACIÓN SOBRE
LA UNIDAD AUDITADA**

El Departamento es una agencia del Gobierno creada por la Sección 6 del Artículo IV de la Constitución. En la Constitución y en la *Ley Núm. 6 del 24 de julio de 1952* se establece el cargo de Secretario de Estado, quien es nombrado por el Gobernador con el consejo y consentimiento del Senado y de la Cámara de Representantes. Este dirige el Departamento.

El Departamento tiene la responsabilidad de fomentar las relaciones culturales, políticas y económicas entre Puerto Rico y países extranjeros, al igual que con otras jurisdicciones de los Estados Unidos de América. Además, realiza diversas funciones de carácter administrativo, tales como:

- Promulgar, publicar, certificar y vender las leyes y los reglamentos del Gobierno de Puerto Rico.
- Reglamentar el uso de la bandera y del escudo de Puerto Rico.
- Expedir licencias para el ejercicio de profesiones u oficios reglamentados por el Estado a través de las juntas examinadoras.
- Preparar y custodiar diversos registros, tales como: cónsules, corporaciones y sociedades, marcas de fábrica, notarios y propiedad intelectual, entre otros.
- Tramitar la solicitud de pasaportes de los ciudadanos de los Estados Unidos, tarea delegada por el Gobierno Federal.
- Coordinar los asuntos de índole protocolar que competen al Gobierno.

Al Secretario de Estado le responde una Subsecretaria. A esta, a su vez, le responde: el Director de Asuntos Legales y Nombramientos, el Director de Auditoría Interna¹, y los secretarios auxiliares de:

- Asuntos de Gobierno
- Asuntos Protocolares y de Comunicación y Prensa

¹ Este puesto quedó vacante el 31 de octubre de 2009 por la implantación de la *Ley 7-2009, Ley Especial Declarando Estado de Emergencia Fiscal y Estableciendo Plan Integral de Estabilización Fiscal para Salvar el Crédito de Puerto Rico*, según enmendada. Al momento de nuestra auditoría, el Departamento contaba con servicios de auditoría provisto por auditores del Departamento de Recreación y Deportes, según el acuerdo interagencial 2011-000013 del 11 de agosto de 2010.

- Relaciones Exteriores
- Administración²
- Juntas Examinadoras
- Servicios³

Las operaciones diarias se llevan a cabo desde dos edificios localizados en el Viejo San Juan: Real Intendencia y Diputación Provincial. El servicio al ciudadano se presta a través del Centro Único de Servicios (CUS) ubicado en el edificio Diputación Provincial, y de las oficinas localizadas en Hato Rey, Arecibo, Guayama y Mayagüez.

Durante los años del 2006 al 2009, el Departamento comenzó a ofrecer a los ciudadanos los servicios de búsqueda en línea para los siguientes registros: Corporaciones, Juntas Examinadoras, Reglamentos, y Marcas y Nombres Comerciales. A partir del 2010, el ciudadano puede efectuar los siguientes procesos en línea, a través de la página en Internet del Departamento:

- Registrar una corporación.
- Radicar el Informe Anual de Corporaciones.
- Solicitar o validar el certificado de *Good Standing*.
- Registrar Marcas y Nombres Comerciales.

La OTC del Departamento cuenta con un Director quien supervisa y dirige las funciones que se realizan en esta oficina, y a este le asiste un Especialista en Tecnología Cibernética. La infraestructura tecnológica del Departamento consiste en una red de área amplia, que agrupa cuatro redes de área local, compuesta por 16⁴ servidores, que se intercomunican, a

² Esta Secretaría tiene bajo supervisión las siguientes cinco oficinas: Recursos Humanos, Compras, Presupuesto y Finanzas, OTC, y Servicios Generales, Transportación y Seguridad.

³ Esta Secretaría tiene bajo su supervisión las siguientes cinco oficinas: CUS, Registro de Transacciones Comerciales, Registro de Marcas y Nombres Comerciales, Registro de Corporaciones, y Certificaciones y Reglamentos.

⁴ Uno de estos servidores pertenece a una compañía privada.

través de *routers*⁵, *switches*⁶ y líneas dedicadas T1. El acceso a Internet es provisto a través de una conexión que mantiene el Departamento con la Oficina de Gerencia y Presupuesto (OGP). Además, el Departamento comparte información del Registro de Transacciones Comerciales y el de Corporaciones con dos proveedores de servicio externo.

El ANEJO contiene una relación de los funcionarios principales del Departamento que actuaron durante el período auditado.

Los gastos operacionales de la OTC eran sufragados del presupuesto operacional del Departamento, que para los años fiscales del 2008-09 al 2010-11 fue de \$14,513,000, \$11,211,000 y \$10,110,000.

El Departamento cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.estado.gobierno.pr>. Esta página provee información acerca de la entidad y de los servicios que presta.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Hon. Kenneth McClintock Hernández, Secretario de Estado, mediante carta de nuestros auditores, del 15 de abril de 2011. En la referida carta se incluyó un anejo con detalles sobre las situaciones comentadas.

Mediante carta del 6 de mayo de 2011, el Secretario de Estado remitió sus comentarios a los hallazgos incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Secretario de Estado para comentarios, por carta del 2 de julio de 2012.

⁵ Dispositivos que distribuyen tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y las tablas de direccionamiento.

⁶ Dispositivos de comunicación central que conectan dos o más segmentos de red y permiten que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

La Lcda. Vanessa Viera Rabelo, Secretaria de Estado Interina, contestó el borrador de los **hallazgos** de este *Informe*, mediante carta del 20 de julio de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OTC del Departamento, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, el acceso lógico a los sistemas de información computadorizados, la continuidad del servicio y la red de comunicaciones se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos 1 y 2** que se comentan a continuación.

Hallazgo 1 - Falta de un plan de seguridad, y de adiestramientos relacionados con la seguridad de los sistemas de información computadorizados

Situaciones

- a. Al 11 de marzo de 2011, el Departamento no tenía un plan de seguridad, aprobado por el Secretario, que incluyera, entre otras cosas, disposiciones en cuanto a:
 - La documentación de la validación de las normas de seguridad⁷
 - La evidencia de un análisis de riesgos, que sea la base del plan de seguridad
 - La responsabilidad de la gerencia, del personal de la OTC y de los demás componentes de la unidad, tales como: los dueños y los usuarios de los recursos de información, el personal a cargo del procesamiento de los datos y los administradores de la seguridad, entre otros
 - Un programa de adiestramiento especializado al equipo clave de seguridad

⁷ La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el análisis de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas, el personal de sistemas de información y los usuarios, y el cual permita mantener los conocimientos actualizados
 - Los procedimientos para informar y responder a incidentes tales como ataques externos e internos, virus y vulnerabilidades que puedan afectar la seguridad de los activos de información de la organización
 - La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).
- b. Al 10 de marzo de 2011, el Director de la OTC y el Especialista en Tecnología Cibernética no habían recibido adiestramientos relacionados con la seguridad de los sistemas de información ni de las normas y los procedimientos aplicables. Estos adiestramientos son necesarios para asegurarse de que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con la seguridad de los sistemas de información.

Crterios

Las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la OGP.

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con este. El mismo debe considerar los sistemas y las instalaciones principales e identificar los deberes de los dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas. **[Apartado a.]**

Efectos

La falta de un plan de seguridad podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos. **[Apartado a.]**

La falta de conocimiento de las normas de seguridad relacionadas con los sistemas de información ocasiona el incumplimiento de las mismas, con los consiguientes efectos adversos en cuanto a la protección de la información y del equipo. Esto, a su vez, podría afectar la integridad, la disponibilidad y la confiabilidad de la información manejada por los usuarios. **[Apartado b.]**

Causas

La situación comentada en el **apartado a.** se atribuye a que el Secretario no había impartido las directrices para que el Director de la OTC preparara un plan de seguridad.

La situación comentada en el **apartado b.** se atribuye a que el Director de la OTC no había identificado, en coordinación con la Directora de Recursos Humanos, las necesidades de adiestramiento del personal de la OTC, en cuanto a los sistemas de seguridad utilizados en el Departamento. Estos adiestramientos deben formar parte, del plan de seguridad de la entidad.

Comentarios de la Gerencia

En la carta de la Secretaria de Estado Interina, esta nos indicó lo siguiente:

Se evaluarán y someterán a la Administración distintos adiestramientos sobre distintos controles de seguridad. *[sic]*
[Apartado a.]

Se está auscultando distintos adiestramientos técnicos relacionados a la seguridad, normas y procedimientos aplicables de los sistemas de información para someterlos a la aprobación de la Administración. *[sic]* **[Apartado b.]**

Véase la Recomendación 1.a. y b.

Hallazgo 2 - Falta de un plan de continuidad de negocios, de pruebas o simulacros para probar la efectividad del Plan de Contingencia, y de acuerdos para mantener un centro alternativo de recuperación de sistemas de información

Situaciones

- a. La OTC del Departamento era responsable de la continuidad de las operaciones de 33 aplicaciones en producción, tales como: Inventario de Equipo Computadorizado, Recursos Humanos, Registro de Corporaciones⁸, Reglamentos, Sistema de Información de Juntas Examinadoras (SIJE), y Registro de Transacciones Comerciales, entre otras.

Al 14 de abril de 2011, el Departamento carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la OTC. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones del Departamento, en caso de riesgos como: inundaciones, variaciones de voltaje y virus de computadoras, entre otros.

- b. El examen efectuado al *Plan de Contingencia (Plan)*⁹ y a las estrategias implantadas por el Departamento para la continuidad de sus operaciones, reveló las siguientes deficiencias:
- 1) No se habían efectuado procedimientos de prueba o simulacros que certificarán la efectividad del *Plan*.
 - 2) El Departamento no contaba con un centro alternativo para restaurar sus operaciones críticas computadorizadas en casos de emergencias. Tampoco había formalizado acuerdos escritos con otra entidad para establecer un centro alternativo en las instalaciones de esta.

⁸ Esta es la base de datos interna que contiene las enmiendas, los cambios, las disoluciones, entre otra información relacionada con las corporaciones registradas en el Departamento. Un proveedor de servicio era responsable de la continuidad de las operaciones relacionadas con el sistema en línea provisto para el Registro de Corporaciones.

⁹ Este tenía fecha de revisión de diciembre de 2009, y fue actualizado en julio de 2012.

Criterios

Las situaciones comentadas en el **apartado a.** son contrarias a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular 77-05*.

Las mejores prácticas en el campo de la tecnología de información establecen que se deben efectuar pruebas o simulacros, por lo menos una vez al año, para certificar la efectividad del *Plan de Contingencia*.

[Apartado b.1)]

Además, como parte integral del plan de contingencias, se sugiere establecer convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la entidad gubernamental, podrían ser los siguientes: **[Apartado b.2)]**

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración
- Un centro alternativo de la propia entidad.

Efectos

Las situaciones comentadas en los **apartados a. y b.1)** podrían propiciar la improvisación, y que en casos de emergencia 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.

La situación comentada en el **apartado b.2)** podría retrasar o impedir una pronta restauración de las operaciones y las funciones administrativas del Departamento, así como el de las aplicaciones que este utiliza para brindar servicios a los profesionales, las corporaciones y al público en general. Esto, porque no tendría disponible unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento.

Causas

La situación comentada en el **apartado a.** se atribuye a que el *Plan* no se había preparado basado en un análisis de riesgos de los sistemas de información computadorizados del Departamento. El avalúo de riesgos se completó en julio de 2012.

La situación comentada en el **apartado b.1)** se debía a que el Secretario no le requirió al Director de la OTC que efectuara pruebas del *Plan* para asegurarse de que este era funcional, y considerara las necesidades y los riesgos del Departamento.

La situación comentada en el **apartado b.2)** se atribuye a que el Director de la OTC no había completado la coordinación del lugar disponible y adecuado que se utilizaría como centro alternativo para restaurar las operaciones críticas computadorizadas del Departamento en casos de emergencias.

Comentarios de la Gerencia

En la carta de la Secretario de Estado Interina, esta nos indicó lo siguiente:

Se está laborando en la recopilación de información para el Plan de Continuidad de Negocio (aunque entendemos está contemplado en el Plan de Contingencia y depende del Centro Alterno de Recuperación de Desastres). [sic] [**Apartado a.**]

Se tratará (por la razón de que la oficina cuenta con dos personas) de diseñar e implantar un proceso de pruebas y/o simulacros para certificar la efectividad del Plan, según recomendado. [sic] [**Apartado b.1)**]

Se envió carta solicitando reunión con el personal técnico de la Oficina de Tecnología de OGP para efectos de coordinar la creación del Centro Alterno de Recuperación de Sistemas de Información. [sic] [**Apartado b.2)**]

Véanse las recomendaciones 1.c. y d., y 2.

RECOMENDACIONES**Al Secretario de Estado**

1. Ver que la Subsecretaria de Estado le requiera a la Secretaria Auxiliar de Administración que supervise eficazmente al Director de la OTC y se asegure de que:
 - a. Prepare un plan de seguridad que incluya los criterios descritos en el **Hallazgo 1-a.**, el cual debe ser remitido al Secretario de Estado para revisión y aprobación. Una vez aprobado, se asegure de que se divulgue a los empleados y a los funcionarios, y se revise periódicamente.
 - b. Efectúe, en coordinación con la Directora de la Oficina de Recursos Humanos del Departamento, un estudio sobre las necesidades de adiestramientos de los funcionarios que tienen a su cargo la seguridad de los sistemas de información del Departamento, y velar por que estos se ofrezcan, para corregir la situación comentada en el **Hallazgo 1-b.**
 - c. Prepare un plan de continuidad de negocios, que cumpla con lo requerido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*, y remita el mismo para la revisión y la aprobación del Secretario de Estado. Una vez estos sean aprobados, tomar las medidas necesarias para asegurarse de que se mantengan actualizados y se conserve una copia en un lugar seguro fuera del Departamento. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados, y que se realicen pruebas periódicas para garantizar la efectividad de los mismos. **[Hallazgo 2-a.]**
 - d. Efectúe las pruebas o los simulacros necesarios para verificar la efectividad del *Plan*, por lo menos una vez al año, y mantenga la documentación de las estrategias utilizadas y de los resultados de las pruebas. **[Hallazgo 2-b.1]**

2. Formalizar un acuerdo escrito con otra entidad que acepte la utilización de sus equipos en casos de desastres o emergencias en el Departamento, o considerar establecer su propio centro alterno en alguna instalación que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OTC. [Hallazgo 2-b.2]

AGRADECIMIENTO

A los funcionarios y a los empleados del Departamento, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor

Por:

Fernando Maldonado

ANEJO

DEPARTAMENTO DE ESTADO
OFICINA DE TECNOLOGÍA CIBERNÉTICA
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Kenneth McClintock Hernández	Secretario de Estado	8 oct. 10	14 abr. 11
Lcda. Vanessa Viera Rabelo	Subsecretaria de Estado	8 oct. 10	14 abr. 11
CPA Marlene Smith Bermúdez	Secretaria Auxiliar de Administración	8 oct. 10	14 abr. 11
Sr. Jaime A. Cuevas Padilla	Director de la Oficina de Tecnología Cibernética	8 oct. 10	14 abr. 11
Sra. Nivia E. Torres Ocasio	Directora de Recursos Humanos	8 oct. 10	14 abr. 11



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-08-32* del 27 de junio de 2008, 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, extensión 2124, 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.

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) 294-0625 o (787) 200-7253, extensión 536.

**INFORMACIÓN DE
CONTACTO***Dirección física:*

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Internet:

<http://www.ocpr.gov.pr>

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069