INFORME DE AUDITORÍA TI-21-11

14 de abril de 2021

Departamento de Recursos Naturales y Ambientales

Oficina de Informática

(Unidad 5280 - Auditoría 14187)

Período auditado: 21 de febrero de 2017 al 31 de mayo de 2018

CONTENIDO

Página

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

14 de abril 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 en la Oficina de Informática del Departamento de Recursos Naturales y Ambientales (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 y de los sistemas de información computadorizados del Departamento se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

1. Determinar si las operaciones de la Oficina de Informática; en lo que concierne a los controles internos para la administración de la seguridad, la continuidad del servicio, el acceso lógico y el uso de las computadoras y los equipos computadorizados; se realizaron, en todos los aspectos significativos, de acuerdo con la reglamentación interna del Departamento y las políticas establecidas 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, entre otras; y si dichos controles eran efectivos.

2. Determinar si las operaciones del Departamento, en lo que concierne a los controles de entrada de datos establecidos para la creación de las cuentas de acceso y a los controles creados por el Comisionado de Navegación para el registro de los marbetes en el Sistema de Información y Registro de Embarcaciones del Comisionado de Navegación (Sistema Neptuno), se efectuaron, en todos los aspectos significativos, de acuerdo con la reglamentación interna del Departamento y las políticas establecidas en la *Carta Circular 140-16*, y si estos controles son efectivos.

3. Determinar si las operaciones del Departamento, en lo que concierne a la implementación del Sistema de Administración de Ruta (SAR) y del Sistema para la Administración del Recurso Agua (SARA), se efectuaron, en todos los aspectos significativos, de acuerdo con los contratos otorgados y los pagos realizados, y con lo establecido en la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad de Gobierno de Puerto Rico*, según enmendada, entre otras.

CONTENIDO DEL INFORME

Este es el segundo y último informe, y contiene siete hallazgos del resultado del examen que realizamos de los objetivos indicados. En el **Anejo 1** presentamos información del primer informe emitido. Ambos informes están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 21 de febrero de 2017 al 31 de mayo de 2018. En algunos aspectos se examinaron transacciones anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos

las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como: entrevistas a funcionarios, exfuncionarios, empleados y contratistas; 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.

Al realizar esta auditoría, utilizamos las *Normas y Procedimientos para la asignación, modificación y cancelación de las cuentas de acceso y para la administración, utilización y mantenimiento de las redes de comunicaciones del Departamento de Recursos Naturales y Ambientales* (*Normas*), aprobadas el 13 de julio de 2005 por el entonces secretario de Recursos Naturales y Ambientales; 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 System Controls Audit Manual* (*FISCAM*)[1] 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 de Recursos Naturales fue creado mediante la *Ley Núm. 23 del 20 de junio de 1972*, según enmendada. El *Plan de Reorganización 1 del 9 de diciembre de 1993 (Plan)* renominó el Departamento como Departamento de Recursos Naturales y Ambientales (Departamento). Este quedó constituido por los siguientes componentes: la Administración de Recursos Naturales, la Administración de Asuntos de

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

Energía[2] y el Consejo Consultivo de Recursos Naturales y Ambientales (Consejo Consultivo). Además, se adscribieron al Departamento, la Autoridad de Desperdicios Sólidos de Puerto Rico, el Comité Asesor sobre Asuntos de Energía, y la Corporación de Recursos Minerales. Sin embargo, estas dependencias gubernamentales operan bajo sus respectivas leyes orgánicas, en la medida en que las disposiciones de estas no sean incompatibles con las que establece el *Plan*.

El Departamento es la dependencia, dentro de la Rama Ejecutiva, responsable de implementar en su fase operacional la política pública y los programas relacionados con el manejo, el desarrollo ambientalmente sostenible, la utilización, el aprovechamiento, la protección y la conservación de los recursos naturales, ambientales y energéticos de la Isla. Esto, de acuerdo con lo dispuesto en la Constitución y en las leyes vigentes de Puerto Rico, y conforme a la política pública ambiental establecida.

El Departamento es dirigido por un secretario nombrado por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico. El secretario es responsable de la dirección general del Departamento y sus componentes. Además, planifica, coordina y supervisa las fases operacionales de las dependencias que lo integran. También prepara el presupuesto y supervisa la utilización de los recursos fiscales, humanos y de equipo.

A la fecha de nuestra auditoría, la estructura organizacional del Departamento estaba compuesta por las oficinas de Oficiales Examinadores, Secretaría, Informática y Recursos Humanos; las secretarías auxiliares de Manejo y Conservación de Áreas Naturales y Biodiversidad, Administración, Educación y Relaciones con la Comunidad, y Permisos, Endosos y Servicios Especializados; las áreas de Recursos de Agua y Minerales, y Planificación Integral; y la

[2] Mediante la *Ley 57-2014, Ley de Transformación y Alivio Energético de Puerto Rico*, entre otras cosas, se creó la Oficina Estatal de Política Pública Energética (OEPPE) y se transfirieron todos los derechos y las obligaciones, el presupuesto, los documentos, los expedientes, los materiales y la propiedad de la Administración de Asuntos de Energía.

Administración de Operaciones Regionales, el Cuerpo de Vigilantes y el Comisionado de Navegación. Además, cuenta con siete oficinas regionales ubicadas en Aguadilla, Arecibo, Guayama, Humacao, Mayagüez, Ponce y San Juan.

Además, la Oficina de Informática estaba compuesta por las divisiones de Infraestructura y Base de Datos, Análisis y Desarrollo de Aplicaciones, Geo Informática y Servicios al Usuario. La Oficina de Informática cuenta con 1 secretaria ejecutiva, 1 gerente de informática de la División de Infraestructura, 1 gerente de informática de la División de Análisis y Desarrollo de Aplicaciones, 1 desarrollador de aplicaciones, 2 técnicos digitalizadores, y 2 técnicos de servicios al usuario y reparaciones. También contaba con 1 gerente de la Oficina de Sistemas de Información de la Junta de Calidad Ambiental (Junta)[3], quien estaba a cargo de los trabajos de la Oficina de Informática del Departamento[4]. Esta Oficina tenía 11 puestos vacantes.

El presupuesto asignado al Departamento proviene de resoluciones conjuntas del Fondo General del Estado Libre Asociado de Puerto Rico, asignaciones especiales, fondos estatales especiales y federales, y otros ingresos. El presupuesto asignado al Departamento durante los años fiscales del 2015-16 al 2017-18, ascendió a $55,754,000, $55,017,000 y $88,243,000[5], respectivamente.

---

[3] Mediante la *Ley 171-2018* se puso en ejecución y dio cumplimiento al *Plan de Reorganización Núm. 10-2018*, el cual transfirió, agrupó y consolidó en el Departamento las funciones de la Junta, entre otras entidades gubernamentales.

[4] Esta designación se realizó al amparo del acuerdo colaborativo 2017-000125, firmado el 30 de junio de 2017 por la secretaria auxiliar de administración del Departamento y la presidenta de la Junta. El mismo es para integrar esfuerzos y unir pericias, destrezas e intereses de ambas agencias para maximizar los recursos de estas y lograr ahorros significativos. Entre los recursos a integrar, se incluyen el Cuerpo de Vigilantes del Departamento, los inspectores y especialistas en Calidad Ambiental, los oficiales de Muestreo y Permisos de la Junta, y el personal administrativo, profesional y de confianza de ambas agencias; siempre y cuando sus funciones no sean conflictivas entre sí.

[5] Los presupuestos de los años fiscales indicados corresponden al Departamento ($51,736,000) y a la Administración de Recursos Naturales ($147,278,000).

La Oficina de Informática no cuenta con un presupuesto propio. Sus gastos son sufragados por el presupuesto del Programa Información y Educación sobre la Protección del Ambiente de la Administración de Recursos Naturales.

El **Anejo 2** 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.drna.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones determinadas durante la auditoría fueron remitidas a la Lcda. Tania Vázquez Rivera, entonces secretaria de Recursos Naturales y Ambientales, mediante cartas del 8 de junio y 3 de julio de 2018. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 3 y 10 de julio de 2018, la licenciada Vázquez Rivera, remitió sus comentarios, los cuales se consideraron al redactar el borrador de este *Informe*.

El 5 de agosto de 2020 remitimos el borrador de este *Informe* al Hon. Rafael A. Marchargo Maldonado, secretario; el borrador de los **hallazgos** de este *Informe* a la licenciada Vázquez Rivera, exsecretaria; y el borrador del **Hallazgo 1** a los exsecretarios Sr. Daniel J. Galán Kercadó, Sr. Javier Vélez Arocho y Sra. Carmen R. Guerrero Pérez.

El 19 de agosto de 2020 el secretario contestó y nos indicó lo siguiente:

> […] Entendemos que los Hallazgos prevalecen y estamos de acuerdo con el Borrador del Informe. Sin embargo, estamos trabajando en implementar las medidas correctivas necesarias para erradicar los Hallazgos establecidos. [*sic*]

La licenciada Vázquez Rivera contestó el 19 de agosto. En los **hallazgos** se incluyeron algunos de sus comentarios.

El señor Vélez Arocho contestó el 28 de agosto, y en el **Hallazgo 1** se incluyeron algunos de sus comentarios.

El señor Galán Kercadó y la señora Guerrero Pérez no contestaron.

CONTROL INTERNO

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

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

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos a 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 del 2 al 7** se comentan las deficiencias de controles internos significativos, dentro del contexto de los objetivos de nuestra auditoría, identificada a base del trabajo realizado.

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

OPINIÓN Y HALLAZGOS

Opinión Cualificada

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

con las normas y la reglamentación aplicables; y que los controles establecidos, relacionados con dichas operaciones, eran efectivos. Esto, excepto por los **hallazgos del 1 al 7** que se comentan a continuación.

Hallazgo 1 - Inversión de fondos públicos en la implementación de sistemas para automatizar los procesos de facturación de la extracción y el uso de agua, y de multas administrativas, que no se utilizaban

Situaciones

a. La política pública del gobierno del Estado Libre Asociado de Puerto Rico establece que las entidades gubernamentales deben realizar sus gastos dentro de un marco de utilidad y austeridad.

Entre julio de 2007 y septiembre de 2012, en el Departamento se iniciaron dos proyectos para implementar sistemas computadorizados para la facturación de la extracción y el uso de agua, y automatizar la recolección de multas. Esto, con el objetivo de proveer a las divisiones de Franquicias de Agua, y Facturación y Cobro; y al Cuerpo de Vigilantes las herramientas necesarias para administrar los permisos de aprovechamiento[6] y facturar el uso de agua de acuerdo con las leyes y la reglamentación vigente.

El Departamento no logró obtener beneficios de la inversión realizada en estos proyectos, ya que los sistemas adquiridos no se utilizaban, según se indica:

1) El 12 de julio de 2007 el Departamento otorgó un contrato a la compañía A para la automatización de los procesos de recolección de lectura de los dispositivos de extracción de agua, la preparación de las facturas correspondientes y la automatización de la recolección de multas.

[6] Es el uso de las aguas de dominio público para usos comunes o privativos. Las aguas de dominio público o el recurso agua son todas las aguas y los cuerpos de agua declarados propiedad y riqueza del Pueblo de Puerto Rico. Para el uso del recurso agua, se necesita un permiso conocido como franquicia. Este es un permiso escrito otorgado por el secretario donde le concede a la franquicia de agua el derecho de utilizar un volumen determinado de agua por un período.

Al 15 de marzo de 2017, luego de una inversión de $66,029 el SAR no se utilizaba. Según nos indicó el director de la División de Facturación y Cobro, el proceso de facturación nunca funcionó.

2) Del 19 de septiembre de 2012 al 30 de septiembre de 2013, el Departamento otorgó un contrato y dos enmiendas a la compañía B para implementar el SARA, que permitiría automatizar y cumplir a cabalidad con los deberes y las metas relacionadas con la administración y el manejo adecuado del recurso agua. El contrato tenía una vigencia del 19 de septiembre al 30 de junio de 2014, y un costo de $174,389, el cual se pagó en su totalidad[7].

El 20 de diciembre de 2012 y el 13 de junio de 2014 el Departamento emitió dos órdenes de compra[8], por $22,533, para la adquisición de equipos, y la activación y el servicio de comunicación de estos. El sistema fue entregado al Departamento el 11 de abril de 2014 e instalado en un servidor en la nube[9]. El 1 de octubre de 2015 la compañía le entregó al oficial principal de informática un disco compacto con el sistema y el 23 de diciembre de 2015 se entregó, mediante correo electrónico, el código fuente y la documentación de este. El 10 de febrero de 2016 se instaló y completó la configuración del sistema.

Al 21 de marzo de 2017, luego de una inversión de $196,922, el SARA no se utilizaba.

Criterio

Las situaciones comentadas son contrarias a lo establecido en el Artículo 2(g) de la *Ley Núm. 230*, según enmendada.

---

[7] De esta cantidad, $1,700 corresponden a la aportación especial del 1.5% establecido por la *Ley 48-2013*.

[8] Una de las órdenes de compra se realizó a la compañía B por $5,453 y la otra compra a la compañía C por $17,080.

[9] Este servidor se encontraba en la nube de una compañía que proveía servicios de almacenamiento y los costos del servicio los pagaba la compañía B.

Efectos

Las situaciones comentadas no permitieron que el Departamento obtuviera el beneficio esperado de los $262,951 invertidos en ambos proyectos. Además, luego de transcurrido 10 años desde el inicio del primer proyecto, el Departamento aún no cuenta con un sistema computadorizado para la facturación del consumo de agua y el manejo de las multas administrativas. Esto, a su vez, priva a las divisiones de Franquicias de Agua, y de Facturación y Cobro de las herramientas necesarias para administrar los permisos de aprovechamiento y facturar el uso de agua. Los procesos para la recopilación de las lecturas sobre el consumo de agua, la facturación y el cobro por el aprovechamiento y uso del agua se realizaban manualmente.

Causas

El director de la División de Facturación y Cobro atribuye lo comentado **apartado a.1)** a que, a pesar de que el sistema permitía el registro de información de las franquicias de agua, este no permitía realizar los procesos de facturación y de preparación de la factura. Además, el sistema era obsoleto, y ya no era compatible con la infraestructura del Departamento, debido a que hubo un cambio en los sistemas de información[10].

Además, el gerente de informática de la División de Análisis y Desarrollo de Aplicaciones de la Oficina de Informática atribuye la situación a que no tuvo participación en la administración y el seguimiento del proyecto para lograr la implementación completa y su continuidad.

El gerente de informática de la División de Análisis y Desarrollo de Aplicaciones de la Oficina de Informática atribuye lo comentado en el **apartado a.2)** a que el sistema entregado por la compañía e instalado en el servidor el 10 de febrero del 2016, no era la versión final del mismo, ya que contenía errores que se habían detectado en las pruebas de calidad.

[10] El SAR estaba diseñado y desarrollado para operar en computadoras con el sistema operativo Windows 2000/XP.

El director de la División de Facturación y Cobro nos indicó que el Departamento se comunicó con la compañía para corregir la situación, se le informó que el tiempo de garantía se había expirado y requería un contrato nuevo.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó, entre otras cosas, lo siguiente:

> […] cuando esta abogada fue nombrada en el mes de enero 2017, como Secretaria del DRNA, el sistema que se discute en el primer hallazgo no estaba operacional según se desprende del mismo informe hace varios años. De mi mejor recuerdo y por información y creencia, entiendo que el área no solicitó que se hiciera una nueva inversión en este sistema. La abogada que suscribe solicitó a las áreas que buscara trabajar en un nuevo sistema electrónico unificado de permisos, multas y facturación para las 4 agencias que por virtud de la Ley 171 de 2 de agosto de 2018, se fusionaron en lo que hoy es el DRNA. Dicho sistema se trabajó a través de propuestas de Alianzas Público-Privadas (APP) con la intención de evitar una inversión adicional de fondos públicos en sistemas que como el SARA que a claras luces y según se desprende del documento objeto de este escrito no fueron funcionales para el DRNA. Al momento de dejar el puesto en el mes de noviembre de 2019, el contrato para una APP que cubría los servicios que se describen en el Hallazgo número 1 del informe de referencia, se encontraban en etapas avanzadas de aprobación. [*sic*]
>
> No es menester resaltar el hecho de que el Hallazgo núm. 1 y las dificultades en el borrador presentados para el mismo, no pasaron en el periodo de tiempo en que esta abogada fungió como Secretaria de DRNA y mas aún no sucedieron en el periodo de tiempo que establece la auditoría realizada. El sistema esta totalmente inoperante antes del 2017. [*sic*]

El señor Vélez Arocho nos indicó, entre otras cosas, lo siguiente:

> Según se plantea […], hubo sistemas que se establecieron y terminaron siendo obsoletos. Lo que no apunta la investigación es la razón de por que no se utilizó el sistema en la nueva administración que entró en el 2012. Ese punto es importante, toda vez que fue durante ese periodo que comenzaron los planes para disolver la unidad principal de la Oficina del Plan de Aguas de Puerto Rico y con ello los esfuerzos de trabajo con el Cuerpo de Vigilantes y demás unidades para el cobro del agua de las franquicias industriales. [*sic*]

Véase la Recomendación 1.

Hallazgo 2 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados y de un procedimiento para el manejo de incidentes de seguridad

Situaciones

a. Un análisis de riesgos es un proceso mediante el cual se identifican los activos de sistemas de información, sus vulnerabilidades y las amenazas a las que se encuentran expuestos. Además, se establecen medidas y controles para evitar o disminuir los riesgos y proteger los activos. Toda entidad gubernamental debe realizar un análisis de riesgos, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

   Al 19 de abril de 2017, en el Departamento no contaba con un informe del análisis de riesgos de los sistemas de información computadorizados.

b. Las entidades gubernamentales deben desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos los límites para estos en términos de tiempo máximo y mínimo de respuesta. Todos los empleados y contratistas deben conocer los procedimientos para informar los diferentes tipos de incidentes.

   Al 7 de julio de 2017, la Oficina de Informática no tenía un procedimiento o plan para el manejo de incidentes, en el que se estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en el Preámbulo y en el Capítulo I de las *Normas*. Además, se aparta de lo establecido en la Sección A. de la *Política ATI-003, Seguridad de los Sistemas de Información*, y a la Sección C. de la *Política ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Lo comentado en el **apartado b.** es contrario a lo establecido en la Sección F. de la *Política ATI-003* y en la Sección E. de la *Política ATI-015* de la *Carta Circular 140-16*.

Efectos

La situación comentada en el **apartado a.** le impide al Departamento estimar el impacto que los elementos de riesgos tendrían sobre los sistemas de información principales utilizadas en sus áreas y programas, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información. Además, dificulta desarrollar un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Departamento, en caso de alguna eventualidad. **[Véase el Hallazgo 3-a.]**

Lo comentado en el **apartado 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. Además, le impide al Departamento tener un control eficaz y documentado sobre el manejo de incidentes.

Causas

El gerente de la División de Infraestructura atribuyó la situación comentada en el **apartado a.** a que el Departamento se encuentra en el proceso de implementación del proyecto de intercomunicación de la infraestructura informática, y el mismo experimenta cambios continuos. Además, atribuyó lo comentado en el **apartado b.** a que la Oficina de Informática no contaba con el personal suficiente para el desarrollo de políticas, procesos y procedimientos.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó, entre otras cosas, lo siguiente:

> […] aunque para el periodo que comprende la auditoría de referencia, el DRNA no había realizado el análisis de riesgos requerido, el mismo se debió a que desde el 2018 entiendo que hasta el presente, debido a la consolidación de agencias que se fusionaron con el DRNA (Junta de Calidad Ambiental,

> Administración de Desperdicios Sólidos y el Programa de Parques Nacionales) se han estado implementando cambios a la infraestructura de los sistemas de información, consolidación de servidores y centro de datos, aplicaciones entre otros. Dicha consolidación y modificación está en proceso por los que se dificulta poder realizar el Análisis de riesgos efectivo y con la certeza requerida. Entiendo, conforme a la información brindada que una vez terminen con la identificación de los nuevos activos fusionados al DRNA, la oficina de informática completará el análisis de riesgo. [*sic*] **[Apartado a.]**

Véanse las recomendaciones 2 y 3.a.1).

Hallazgo 3 - Falta de un plan de continuidad de negocios, deficiencias relacionadas con el plan de contingencias, y falta de un centro alterno para la recuperación de las operaciones computadorizadas

Situaciones

a. Las entidades gubernamentales deben desarrollar un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones basado en un análisis de riesgo. Estos planes deben establecer, entre otras cosas, las estrategias de respuesta, recuperación, reanudación y restauración para todos los procesos principales de la agencia. Además, deben ser actualizados cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

   Al 7 de julio de 2017, el Departamento carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de sus sistemas de información computadorizados.

b. Toda entidad gubernamental debe contar con un plan de contingencias, para restablecer sus operaciones más importantes en caso de que surja una emergencia. Dicho plan debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de los sistemas de información computadorizados.

Al 5 de julio de 2017, el Departamento contaba con el *Plan de Contingencia Interno Contra Desastres Naturales (Plan de Contingencia)*, el cual tenía como propósito establecer las medidas preventivas para proteger el personal, el equipo, los materiales y los documentos. El examen realizado al mismo reveló lo siguiente:

1) No contaba con fecha de aprobación ni la firma de los secretarios en funciones.

2) No incluía los siguientes requisitos necesarios para atender situaciones de emergencia:

   - Los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información de los usuarios.

   - El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones. El *Plan de Contingencia* indicaba que el inventario se encontraba en proceso.

   - Un itinerario de restauración que incluya los procedimientos para restaurar los respaldos.

   - El detalle de la configuración de los equipos críticos (equipo de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos.

3) No tenía actualizado los nombres de los empleados de la Oficina de Informática; las oficinas regionales; los equipos computadorizados y de comunicación existentes; y el itinerario de restauración. Este último incluía tareas a realizarse en el centro alterno cuando el Departamento no contaba con uno.

c. Como parte integral del plan de continuidad de negocios, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse, además, 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, podrían ser una entidad

pública o privada de similar configuración y tamaño; una compañía dedicada a servicios de restauración; o un centro alterno de la propia entidad.

Al 19 de abril de 2017, el Departamento no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

Situaciones similares a las comentadas en los **apartados b. y c.** fueron comentadas en el *Informe de Auditoría TI-03-07* del 8 de abril de 2003.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la Sección B de la *Política ATI-003*, Sección B de la *Política ATI-004, Servicios de Tecnología*, y Sección E de la *Política ATI-015*, de la *Carta Circular 140-16*.

Lo comentado en los **apartados b. y c.** es contrario a lo establecido en el Capítulo IV, Sección 6, inciso o de las *Normas*, y en el Capítulo 3.5, *Contingency Planning*, del *FISCAM*.

Efectos

Las situaciones comentadas en los **apartados a. y b.** pueden 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 ofrecidos a los usuarios y a los clientes del Departamento.

La situación comentada en el **apartado c.** podría afectar las operaciones del Departamento, ya que no tendría disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales del Departamento.

Causas

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a la falta de un análisis de riesgos de los sistemas de información computadorizados que sirva de base para la preparación y la revisión de los mencionados planes. **[Véase el Hallazgo 2-a.]**

El gerente de la División de Infraestructura atribuyó la situación comentada en el **apartado a.** a que el Departamento no contaba con el personal y el tiempo para definir y realizar los requerimientos mínimos para desarrollar el plan. Además, atribuye la situación comentada en el **apartado c.** a que la Oficina de Informática no había identificado un lugar disponible y adecuado como centro alterno para su utilización en caso de emergencia. Para el 2016, el oficial principal de informática había solicitado cotizaciones a varias compañías, pero este no logró seleccionar un lugar ni establecer un acuerdo.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó, lo siguiente:

> El Hallazgo 3 establece que, a la fecha del 5 de julio de 2017, el Plan de Contingencias Interno Contra Desastres Naturales (Plan de Contingencias) se encontraba incompleto. En este caso, es de mi mejor recuerdo que dicho Plan, luego de los huracanes Irma y María, en conjunto a la fusión de la Agencia luego del agosto 2018, se estaba revisando y reescribiendo. [*sic*] **[Apartado b.]**

Véase la Recomendación 3 de la a.2) a la b.

Hallazgo 4 - Deficiencias con la configuración de la política de contraseñas y la administración de las cuentas de acceso

Situaciones

a. En las *Normas* se establece que los usuarios del Departamento deben utilizar un sistema de contraseñas robusto, compuestas de un mínimo de ocho caracteres y una combinación de letras y números.

El Departamento contaba con 16 servidores físicos y 42 virtuales, entre los que se encontraba el servidor principal[11]. El examen efectuado el 17 de mayo de 2017 sobre los parámetros de seguridad y los controles de acceso establecidos en el sistema operativo del servidor principal reveló que en este no se había definido la política de contraseñas para requerir que estas estuvieran compuestas por, al menos, 8 caracteres (*minimum password length*).

b. Las cuentas de acceso del Departamento deben quedar automáticamente suspendidas después de un período de inactividad, que se recomienda sea de 30 días. Además, los privilegios de acceso concedidos a los usuarios deben ser ratificados cada 6 meses. Se debe revocar rápidamente la cuenta o los privilegios de un usuario cuando se reciba la notificación del supervisor y, en particular, cuando un empleado cese en sus funciones. Para las personas que no son empleados del Departamento, las cuentas de acceso deberán estar autorizadas y deben expirarse automáticamente después de 30 días.

    1) Al 11 de julio de 2017, en el servidor principal había 702 cuentas de usuarios activas para acceder a la red. El examen de estas cuentas reveló las siguientes deficiencias:

        a) Doscientas sesenta cuentas (37%) permanecían activas a pesar de que tenían más de 30 días de inactividad.

            (1) Para 152 de estas cuentas (58%), habían transcurrido entre 33 y 3,189 días desde la fecha de su último acceso (*last logon*).

            (2) Las restantes 108 cuentas (42%) no se habían utilizado desde la fecha que fueron creadas. Habían transcurrido entre 47 y 4,165 días desde la fecha de su creación.

        b) A dos cuentas de acceso creadas para dos compañías externas, no se les había configurado una fecha de expiración.

[11] Este servidor está configurado como controlador de dominio.

c) Al 11 de julio de 2017, no se había inactivado del servidor principal las cuentas de acceso asignadas a 7 empleados que cesaron en sus funciones entre el 15 de mayo de 2016 y el 30 de junio de 2017.

2) El examen efectuado el 11 de agosto de 2017 sobre las cuentas de acceso de los usuarios del Sistema de Información de Permisos y Endosos Mecanizado, reveló que no se habían eliminado las cuentas de acceso de 24 exempleados. Esto, a pesar de haber transcurrido entre 192 y 4,605 días desde el cese de sus funciones.

Criterio

Las situaciones comentadas se apartan de lo establecido en los capítulos II y IV de las *Normas*.

Efectos

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

Causas

Las situaciones comentadas en los **apartados a. y b.1)** se debían a que la Oficina de Informática no contaba con el puesto de administrador de seguridad ni contaba con personal suficiente. El gerente de informática de la División de Infraestructura dirigía las divisiones de Infraestructura y de Servicio al Usuario, por lo que administraba las telecomunicaciones, los servidores y la red de sistemas de información y configuraba las instalaciones del Departamento. Además, creaba las cuentas de acceso de la red del Departamento. Por esto, se le hacía difícil configurar los parámetros de seguridad y administrar las cuentas de los usuarios del Departamento.

Las situaciones mencionadas en el **apartado b.1)c) y 2)**, obedecen a que los funcionarios responsables de las mismas se apartaron de lo establecido en las *Normas* indicadas.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó, lo siguiente:

> De mi mejor recuerdo dicho señalamiento fue corregido toda vez que la política para requerir las contraseñas en el sistema se modificó para que la misma incluyera más caracteres y complejas combinaciones. Asimismo, conforme a la información brindada se estableció un plan de auditoría de cuentas de determinados períodos para actividades irregulares y poder tener mayor control. [*sic*]

Consideramos las alegaciones de la exsecretaria, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que no se nos suministró evidencia sobre la corrección de la política de contraseñas ni el plan de auditorías para detectar actividades irregulares de las cuentas.

Véanse las recomendaciones 3.c. y 4.

Hallazgo 5 - Falta almacenamiento de los respaldos fuera de los predios del Departamento

Situación

a. En el Departamento deben realizarse, periódicamente, respaldos de los datos guardados en las computadoras y los servidores. Las copias de estos respaldos deben almacenarse en un lugar seguro. Además, los programas y datos esenciales para la operación del Departamento deben guardarse en un lugar distante a sus oficinas centrales.

   En marzo de 2017 el Departamento contaba con 16 servidores físicos y 42 virtuales, ubicados en el Centro de Cómputos. Al 11 de mayo de 2017, el gerente de informática de la División de Infraestructura realizaba respaldos a 32 de los servidores virtuales.

   Al 11 de mayo de 2017, no se mantenían copias de estos respaldos en un lugar seguro fuera de los predios del Departamento.

   Una situación similar fue comentada en el *Informe de Auditoría TI-03-07*.

Criterio

La situación comentada se aparta de los establecido en el Inciso 25 del Capítulo II de las *Normas*.

Efecto

La situación comentada puede ocasionar que, en casos de emergencias, el Departamento no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Causa

El gerente de la División de Infraestructura atribuyó la situación comentada a que la Oficina de Informática no contaba con la capacidad para transportar o exportar los respaldos a un lugar externo fuera de los predios del Departamento.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó lo siguiente:

> En cuanto a este señalamiento, al momento de esta servidora, terminara sus funciones en el DRNA, se estaba cotizando un sistema de respaldo de datos para la información del DRNA incluyendo los datos de las tres Agencias que eran parte del proceso de fusión por virtud de la Ley 171 de 2018. [*sic*]

Véase la Recomendación 3.d.

Hallazgo 6 - Falta de documentación de la justificación y la autorización de los accesos a las cuentas con privilegios de administrador

Situaciones

a. La información y los programas de aplicación utilizados en las operaciones de las entidades gubernamentales deben tener controles de acceso para su utilización, de manera que solamente el personal autorizado pueda ver los datos necesarios, o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deben incluir mecanismos de autenticación y autorización. En las *Normas* del Departamento se establece que toda solicitud para una cuenta nueva o el cambio de privilegios debe realizarse por escrito y aprobarse por la Oficina de Informática.

Al 10 de agosto de 2017, el personal de la Oficina de Informática no suministró para examen los documentos justificantes y de autorización para otorgar los privilegios de administrador de los sistemas operativos a los gerentes de informática de las divisiones de Infraestructura, y de Análisis y Desarrollo de Aplicaciones; el desarrollador de aplicaciones; y dos técnicos de servicio al usuario y reparaciones.

Estos amplios privilegios permiten, entre otras cosas, realizar cambios a la configuración del sistema, instalar programas y equipos, acceder a todos los archivos de la computadora y realizar cambios a las cuentas de otros usuarios.

Criterios

La situación comentada es contraria a lo establecido en el Inciso 5.b del Capítulo IV de las *Normas* y en la Sección E.3 de la *Política ATI-003* de la *Carta Circular 140-16*.

Efectos

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios. También pueden propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta; y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causa

Lo comentado se debía principalmente a que el gerente de informática de la División de Infraestructura desconocía si la solicitud y creación de las cuentas de administrador fue documentada.

Véase la Recomendación 3.e.

Hallazgo 7 - Falta de un inventario de la propiedad actualizado y de un registro de programas instalados en las computadoras

Situaciones

a. Los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, deben constar en el inventario de las respectivas agencias y solo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente y constatarse en un documento oficial.

   Además, la Oficina de Propiedad debe mantener registros de inventarios completos y actualizados.

   1) Al 19 de junio de 2017, el Departamento no contaba con un inventario actualizado que incluyera los equipos computadorizados.

   2) Al 28 de abril de 2017, la Oficina de Informática no mantenía un registro de los programas adquiridos e instalados en cada computadora.

   Situaciones similares fueron comentadas en los informes de auditoría *DA-13-46* del 28 de abril de 2013 y *TI-03-07* del 8 de abril de 2003.

Criterios

La situación comentada en el **apartado a.1)** es contrario a lo establecido en el Inciso 7 del Capítulo II de las *Normas*.

Lo comentado en el **apartado a.2)** se aparta de lo establecido en la *Política ATI-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la *Carta Circular 140-16*.

Efectos

La situación comentada en el **apartado a.1)** le impide al Departamento mantener un control efectivo sobre el equipo y la propiedad bajo su

custodia. Además, propicia el ambiente para el uso indebido o la desaparición de la propiedad, y otras situaciones adversas, sin que se puedan detectar a tiempo para fijar responsabilidades.

La situación comentada en el **apartado a.2)** impide ejercer un control eficaz de los programas y de las licencias correspondientes. Además, puede propiciar la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para el Departamento.

Causas

El director de la División de Servicios Generales atribuyó la situación comentada en el **apartado a.1)** a que el Departamento no contaba con un programa computadorizado para registrar el inventario. En el 2012 se adquirió un sistema de base de datos para registrar la propiedad mueble, el cual no había sido instalado.

El gerente de la División de Infraestructura atribuyó lo comentado en el **apartado a.2)** a que en el Departamento no se mantenía un control de las compras de programas y equipos computadorizados, por lo que, en muchas ocasiones, estos se entregaban directamente al usuario final, sin notificar u obtener la autorización de uso de la Oficina de Informática.

Comentarios de la Gerencia

La licenciada Vázquez Rivera nos indicó lo siguiente:

> Dicho señalamiento debe ser corregido con el nuevo programa electrónico que se estaba trabajando a modo de APP en el DRNA al momento de terminar mis funciones. Dicha plataforma de mi mejor recuerdo provee el espacio para mantener un inventario electrónico de todos los bienes de la Agencia, incluyendo las Agencias que se fusionan con el DRNA, esto sin un costo mayor al erario. [*sic*]

Véanse las recomendaciones 3.f. y 5.

RECOMENDACIONES

Al secretario de Recursos Naturales y Ambientales

1. Tomar las medidas necesarias para que no se repitan situaciones como las que se comentan en el **Hallazgo 1**. Entre otras medidas, debe asegurarse de que, para futuros proyectos de implementación de sistemas de información computadorizados se cumpla con lo siguiente:

    a. Realizar una planificación adecuada que considere, entre otras cosas, las necesidades de tecnología y las particularidades operacionales del Departamento; la infraestructura existente; y los recursos y costos necesarios para lograr la implementación exitosa y la continuidad del sistema.

    b. Identificar al personal del Departamento que será responsable de la administración y el seguimiento de los sistemas para lograr la implementación exitosa y la continuidad de estos. Esto incluye, entre otras cosas, la supervisión del personal interno y externo para que se completen los trabajos en las fechas establecidas y se cumplan los objetivos establecidos; y la verificación de los trabajos completados para asegurarse de que cumplen con los requisitos establecidos en las propuestas.

2. Asegurarse de que se realice y se documente el análisis de riesgos de los sistemas de información computadorizados del Departamento, según se establece en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*. El mismo debe ser un informe gerencial y remitirse para su revisión y aprobación. Además, una vez aprobado, ver que se revise cada vez que surja un cambio significativo dentro de la infraestructura operacional y tecnológica del Departamento, para asegurarse de que se mantenga actualizado. **[Hallazgo 2-a.]**

3. Asegurarse de que el oficial principal de informática del Departamento cumpla con lo siguiente:

    a. Identifique alternativas costo-efectivas para preparar y remitir, para su aprobación los siguientes documentos:

        1) El procedimiento para el manejo de incidentes. Como parte de este, debe requerirse que se documenten todos los incidentes y se indique cómo se resolvieron. Esto, de manera que, cuando dichos incidentes se repitan, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información computadorizados y la continuidad de las operaciones. **[Hallazgo 2-b.]**

        2) El plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones, según se establece en la *Política ATI-003*. El mismo deberá estar basado en un análisis de riesgos. Una vez este sea aprobado, asegurarse de que se realicen pruebas periódicas para garantizar la su efectividad, y se divulgue a los empleados y a los funcionarios concernientes. Además, se mantenga una copia de este plan en un lugar seguro fuera de lo predios del Departamento. **[Hallazgo 3-a.]**

        3) Un plan de contingencias actualizado y que incluya los aspectos comentados en el **Hallazgo 3-b.**

    b. Identifique un centro alterno que no esté expuesto a los mismos riesgos que el área de sistemas de información, y que cuente con la infraestructura y los equipos necesarios para restaurar las operaciones críticas computadorizadas del Departamento en caso de emergencia. **[Hallazgo 3-c.]**

c. Efectúe las modificaciones en los parámetros de seguridad del sistema operativo del servidor principal de la red para lo siguiente:

1) Requerir, al menos, ocho caracteres para la utilización de las contraseñas, según establecido en las *Normas* y la *Política ATI-003*. **[Hallazgo 4-a.]**

2) Evaluar las cuentas de acceso con más de 30 días de inactividad mencionadas en el **Hallazgo 4-b.1)a)** para identificar cuáles de estas no son necesarias para las operaciones del Departamento y sus sistemas de información, y realizar las gestiones necesarias para eliminar o modificar el privilegio de acceso de estas.

3) Desactivar las cuentas de acceso de los exempleados y contratistas que concluyan sus labores en el Departamento, y ver que, en lo sucesivo, las cuentas se desactiven en el momento en que el usuario cese sus funciones. **[Hallazgo 4-b.1)b) y c), y 2)]**

d. Almacene una copia de los respaldos en un lugar seguro. Este no debe estar expuesto a las mismas amenazas de desastre que la Oficina Central, en donde se encuentran los servidores ubicados en la Oficina de Informática y el servidor en donde se graban los respaldos del Departamento. **[Hallazgo 5]**

e. Documente la justificación y autorización de la asignación de los privilegios de administrador de los sistemas operativos a los gerentes de informática de las divisiones de Infraestructura, y de Análisis y Desarrollo de Aplicaciones; el desarrollador de aplicaciones y cualquier otro usuario que requiera de estos privilegios. **[Hallazgo 6]**

f. Realice las gestiones necesarias para lo siguiente:

1) Evaluar la posibilidad de implementar el sistema computarizado que se adquirió en el 2012, para registrar la propiedad mueble. **[Hallazgo 7-a.1)]**

2) Preparar y mantener actualizado un registro de los programas adquiridos e instalados en las computadoras del Departamento. Este registro debe incluir, entre otras cosas, el número de licencia de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde estaban instalados los programas, y el costo de los programas instalados. **[Hallazgo 7-a.2)]**

4. Asegurarse de que la directora de la Oficina de Recursos Humanos notifique a la Oficina de Informática tan pronto un empleado cese en sus funciones, de manera que se cancele la cuenta de acceso a los sistemas de información del Departamento. **[Hallazgo 4-b.1)c) y 2)]**

5. Asegurarse de que el director de la División de Servicios Generales

a. Realice un inventario de los activos fijos que incluya los equipos computadorizados del Departamento. **[Hallazgo 7-a.1)]**

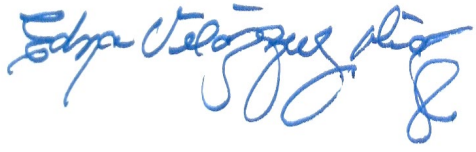
b. Envíe copia del recibo de propiedad al OPI, en casos de equipos o programas tecnológicos adquiridos por la entidad, para que este pueda preparar el registro comentado en el **Hallazgo 7-a.2)**.

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 1

DEPARTAMENTO DE RECURSOS NATURALES Y AMBIENTALES
OFICINA DE INFORMÁTICA

INFORME PUBLICADO

INFORME	FECHA	CONTENIDO DEL INFORME
TI-19-09	3 jun. 19	Resultado del examen de la utilización de las opciones, los controles para la validación de las asistencias registradas, y la realización y documentación de los ajustes del Sistema Kronos del Departamento

ANEJO 2

DEPARTAMENTO DE RECURSOS NATURALES Y AMBIENTALES
OFICINA DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcda. Tania Vázquez Rivera	Secretaria	21 feb. 17	31 may. 18
Sr. Armando G. Otero Pagán	Subsecretario	15 mar. 18	31 may. 18
Vacante	"	21 feb. 17	14 mar. 18
Sr. Osvaldo Alomar Otero	Supervisor Oficina de Informática[12]	18 abr. 18	31 may. 18
Sra. Ana M. Ramos Vaquero	Oficial Principal de Informática, Interina	14 mar. 17	17 abr. 18
Vacante	"	21 feb. 17	13 mar. 17

[12] Véase la nota al calce 3.

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

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr