**INFORME DE AUDITORÍA TI-15-07**

17 de febrero de 2015

**Administración de Terrenos de Puerto Rico**

**Centro de Información**

(Unidad 5005 - Auditoría 13811)

Período auditado: 18 de febrero de 2013 al 19 de febrero de 2014

**CONTENIDO**

**Página**

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

17 de febrero de 2015

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

Realizamos una auditoría de las operaciones del Centro de Información de la Administración de Terrenos de Puerto Rico (Administración) 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 18 de febrero de 2013 al 19 de febrero de 2014. En algunos aspectos se examinaron transacciones de fechas anteriores. 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 *Informe* contiene siete hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, el acceso lógico, la continuidad del servicio y la red de comunicación. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

**INFORMACIÓN SOBRE LA UNIDAD AUDITADA**

La Administración fue creada por virtud de la *Ley Núm. 13 del 16 de mayo de 1962*, según enmendada, para promover de forma planificada el bienestar de la comunidad puertorriqueña, mediante gestiones y programas diseñados para lograr el uso eficiente de los terrenos en Puerto Rico en la forma más amplia y económica posible. Además, para garantizar las reservas de terrenos adecuadas para ayudar al Gobierno a realizar su política pública de desarrollo industrial, comercial y social, y proveer para su mantenimiento y custodia.

El 22 de junio de 1994, mediante el *Plan de Reorganización 4*, se enmendó la *Ley Núm. 13*, para agrupar y agilizar el funcionamiento de varias entidades gubernamentales que tienen funciones de planificar, de promover y de fomentar iniciativas de desarrollo económico para Puerto Rico. Mediante dicho *Plan*, se adscribió la Administración al Departamento de Desarrollo Económico y Comercio (Departamento) como un componente operacional. Se dispuso que la Administración continuaría operando bajo la *Ley Núm. 13*, excepto que el Secretario del Departamento sustituyera al Gobernador como Miembro y Presidente de la Junta de Gobierno de la Administración (Junta). También se dispuso que el Gobernador nombra al Director Ejecutivo con el consejo y consentimiento del Senado, y le fija su sueldo. Este funcionario le responde a la Junta.

Los poderes de la Administración son ejercidos por la Junta, quien determina la política general de la Administración. La Junta está compuesta por el Secretario del Departamento, quien es el Presidente; el Presidente de la Junta de Planificación de Puerto Rico, quien es el Vicepresidente; los secretarios de Hacienda, de Transportación y Obras Públicas, de Vivienda y de Agricultura; el Director Ejecutivo de la Compañía de Fomento Industrial de Puerto Rico; y dos representantes del sector privado que son nombrados por el Gobernador, con el consejo y consentimiento del Senado.

La Oficina del Director Ejecutivo, en el desempeño de sus responsabilidades, cuenta con un Subdirector. Para cumplir con sus funciones, la Administración cuenta, principalmente, con las oficinas de

Servicios Legales, de Auditoría Interna, de Programa de Desarrollo y Usos de Terrenos, de Recursos Humanos y Relaciones Laborales, de Presupuesto y Finanzas, de Ingeniería, de Servicios Generales, y de Administración de Propiedades; y el Centro de Información.

A la fecha de nuestra auditoría, el Centro de Información era dirigido por un Administrador, el cual le respondía al Director Ejecutivo de la Administración, y contaba con un puesto de Oficial de Sistemas de Información, el cual estaba vacante.

La Administración, para sus operaciones, cuenta con una red de área local (LAN, por sus siglas en inglés) que da servicio a sus oficinas y áreas ubicadas en el primer y segundo piso del edificio. Esta consiste de 8 servidores físicos y 3 virtuales, 6 *switches*[1] CISCO, y 65 computadoras.

Los recursos para financiar las actividades operacionales de la Administración provienen principalmente del arrendamiento y de la venta de sus inmuebles. Para los años fiscales del 2011-12 al 2013-14, el presupuesto de la Administración ascendió a $31,556,740, $21,556,653 y $21,502,987, respectivamente. Para los años fiscales del 2011-12 al 2013-14, se asignaron fondos a la partida 1.1-028 Plan de Mecanización, ascendentes a $259,004.

La Administración cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.terrenos.pr.gov. 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* y otras situaciones determinadas durante la auditoría, relacionadas con los controles internos establecidos para la administración del programa de seguridad, el acceso lógico, la segregación de funciones, la continuidad del servicio, el desarrollo y control de cambios de las aplicaciones y la red de comunicación fueron remitidas al Agro. Luis Rivero Cubano,

[1] 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.

Director Ejecutivo de la Administración, mediante carta de nuestros auditores, del 28 de marzo de 2014. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

El 29 de abril de 2014 el Director Ejecutivo remitió sus comentarios sobre los hallazgos incluidos en la carta de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió para comentarios al agrónomo Rivero Cubano, Director Ejecutivo, y a la Sra. María de L. Blázquez Arsuaga, ex Directora Ejecutiva de la Administración, mediante cartas del 21 de noviembre de 2014. En este se indicaron datos específicos, tales como: nombres de servidores, de aplicaciones y de compañías, los cuales por seguridad no se incluyen en este *Informe*.

El 5 de diciembre de 2014 el Director Ejecutivo solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 8 de diciembre le concedimos la prórroga hasta el 22 de diciembre.

El Director Ejecutivo contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 19 de diciembre de 2014. Sus comentarios fueron considerados en la redacción final de este *Informe*. En los **hallazgos** se incluyeron algunos de sus comentarios.

El 1 de diciembre de 2014 la ex Directora Ejecutiva solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 2 de diciembre le concedimos la prórroga hasta el 15 de diciembre. La ex Directora Ejecutiva contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 16 de diciembre. Esta indicó que no tenía comentarios sobre las situaciones presentadas, y solicitó que corrigiéramos el puesto ocupado por una funcionaria en el anejo de los funcionarios principales de la entidad incluido en el borrador de este *Informe*.

## OPINIÓN Y HALLAZGOS

### Opinión favorable con excepciones

Las pruebas efectuadas revelaron que las operaciones del Centro de Información, en lo que concierne a los controles establecidos para la administración del programa de seguridad, el acceso físico y lógico, la

segregación de funciones, la continuidad del servicio, el desarrollo y control de cambios de las aplicaciones, la red de comunicación y las computadoras, se realizaron sustancialmente de acuerdo con las normas generalmente aceptadas en este campo; excepto por los **hallazgos del 1 al 7** que se comentan a continuación.

**Hallazgo 1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados y de un análisis de impacto de negocio**

**Situaciones**

a. El análisis de riesgos de los sistemas de información computadorizados es un proceso a través del cual se identifican los activos de sistemas de información computadorizados existentes en una entidad, sus vulnerabilidades, y las amenazas a las que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas. Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implantados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, y proteger dichos activos, de manera que no se afecten adversamente las operaciones de la entidad. Mediante este proceso se asegura que las medidas de seguridad y los controles a ser implantados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

   Al 12 de febrero de 2014, en la Administración no se había preparado el informe del análisis de riesgos de los sistemas de información computadorizados.

b. El análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por la pérdida o la interrupción de las operaciones, y de las vulnerabilidades y las amenazas que fueron identificadas y clasificadas en el análisis de riesgos. Además, debe proveer información para determinar las estrategias de recuperación más apropiadas. Al 8 de marzo de 2013, en la Administración no se había realizado un análisis de impacto de negocio sobre los sistemas de información computadorizados.

**Criterios**

La situación comentada en el **apartado a.** se aparta de lo establecido en el *ATDI-600, Plan de Contingencias y Seguridad de la Información*, del *Manual de Políticas y Procedimiento de la Oficina del Centro de Información (Manual)*, aprobado el 28 de abril de 2005 por el Director Ejecutivo de la Administración. En este se establece, entre otras cosas, que para asegurar que se consideran todas las posibles eventualidades, durante el desarrollo del plan de contingencias, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual, se deberá realizar un análisis de riesgos.

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 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 Oficina de Gerencia y Presupuesto (OGP); y de la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el Director de la OGP.

**Efectos**

Las situaciones comentadas impiden a la Administración estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificultan 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 de la Administración, en caso de que surja alguna eventualidad. **[Véase el Hallazgo 2-a.]**

**Causas**

Las situaciones comentadas se atribuyen a que el Administrador del Centro de Información desconocía cómo se preparaban los análisis de riesgos y de impacto de negocios requeridos en el *ATDI-600*, y en las políticas *TIG-003* y *TIG-015*.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos, una vez recibido el 1er Borrador de los Hallazgos en Marzo 2014, contrato a la compañía […] (consultores) para que asistiera al Administrador del Centro de Información al desarrollo e implementación del análisis de riesgos de los sistemas computadorizados de la Administración, esto con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1 y 2.**

**Hallazgo 2 - Falta de un plan de continuidad de negocios, de un plan de contingencias sobre los sistemas de información y de un centro alterno para la recuperación de las operaciones computadorizadas**

**Situaciones**

a. Al 12 de febrero de 2014, la Administración carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados del Centro de Información. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la Administración, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red de comunicaciones (red), o desastres naturales, entre otros.

b. La Administración carecía de un plan de contingencias para los sistemas de información, que incluyera los siguientes requisitos que son necesarios para atender situaciones de emergencia:

- Los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información de los usuarios que acceden los sistemas de información mediante conexiones remotas
- El inventario actualizado de los equipos, de los sistemas operativos y de las aplicaciones
- La identificación de los archivos críticos de la Administración
- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y 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
- El nombre del encargado de activar el plan y del personal de reserva, de forma tal que pueda ser ejecutado sin depender de individuos específicos
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia
- Una lista de los números de teléfonos de los miembros de cada grupo de recuperación.

c. La Administración no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia. Tampoco había formalizado acuerdos escritos con otra entidad para establecer un centro alterno en las instalaciones de esta.

Una situación similar a la del **apartado a.** fue comentada en el *Informe de Revisión de Controles en los Sistemas de Información* emitido el 20 de agosto de 2010 por un consultor externo.

**Criterios**

Las situaciones comentadas en los **apartados a. y b.** son contrarias a lo establecido en las políticas *TIG-003* y *TIG-004, Servicios de Tecnología*, de la *Carta Circular 77-05*, y *TIG-015*.

La situación comentada en el **apartado b.** se aparta de lo establecido en el *ATDI-600* del *Manual*. En este se establecen unas guías para desarrollar un plan de contingencias con el propósito de confrontar un desastre, y poder continuar con la misión de la agencia por un tiempo indeterminado.

Las mejores prácticas en el campo de la tecnología de información sugieren que como parte integral del plan de continuidad de negocios, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. 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 agencia, podrían ser los siguientes: **[Apartado c.]**

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

**Efectos**

Las situaciones comentadas en los **apartados a. y b.** pueden 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 y de interrupciones prolongadas de los servicios ofrecidos a los usuarios de la Administración.

La situación comentada en el **apartado c.** podría afectar las funciones de la Administración y los servicios del Centro de Información, ya que no tendrían 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 Centro de Información.

**Causas**

La situación comentada en el **apartado a.** se atribuye a que en la Administración se contrató a una compañía para elaborar y desarrollar un plan operacional de emergencias que cumpliera con el *Boletín Administrativo 2009-043*[2], y esta no había finalizado la preparación del mismo.

Lo comentado en el **apartado b.** se atribuye a que el Administrador del Centro de Información entendía que con el *ATDI-600* del *Manual* se cumplía con el requisito de tener un plan de contingencias. Sin embargo, el *ATDI-600* es una guía de cómo se debe preparar un plan de contingencias.

La situación comentada en el **apartado c.** se atribuye a que el Director Ejecutivo no le había requerido al Administrador del Centro de Información que realizara las gestiones necesarias para identificar un centro alterno disponible y adecuado para restaurar las operaciones críticas computadorizadas de la Administración.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos, una vez recibido el 1er Borrador de los Hallazgos en Marzo 2014, contrato a la compañía […] (consultores) para que asistiera al Administrador del Centro de Información al desarrollo e implementación del plan de continuidad de negocio y de un plan de contingencias sobre los sistemas computadorizados de la Administración, esto con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1, 3.a. y b.1), y 4.**

[2] Orden Ejecutiva del Gobernador para establecer normas sobre la coordinación de funciones ejecutivas en el manejo de emergencias emitido el 9 de noviembre de 2009.

**Hallazgo 3 - Deficiencias relacionadas con el almacenamiento y la retención de los respaldos de información en la bóveda externa**

**Situación**

a. En el *ATDI-401, Procedimiento de Manejo y Administración de Inventario de Copias de Resguardo*, del *Manual*, se establecen los controles para el manejo y la administración de las copias de respaldo que son originadas en la Administración y todo aquel material informativo de carácter confidencial o cualquier documento que sea almacenado en la bóveda exterior por el Centro de Información.

El Administrador del Centro de Información es responsable de preparar los respaldos, mediante la aplicación *Windows Backup*, del archivo que contenía los documentos de los usuarios y de las bases de datos de la aplicación financiera, utilizada en la Oficina de Presupuesto y Finanzas. Los respaldos son producidos en discos externos y enviados a una bóveda externa ubicada en las instalaciones de una compañía, con el propósito de mantenerlos en un lugar seguro fuera de los predios donde están ubicados los servidores de la Administración.

La inspección realizada el 27 de septiembre de 2013 al contenido de la bóveda externa reveló lo siguiente:

1) No se encontraron los respaldos de los años naturales 2008, 2009, 2010 y 2012.

2) No se encontraron los respaldos de los años fiscales del 2007-08 al 2011-12.

3) Los respaldos mensuales no se conservaban en la bóveda externa.

**Criterio**

Las situaciones comentadas son contrarias a lo establecido en el *Procedimiento ATDI-401* del *Manual*. En este se establece, entre otras cosas, que se realizarán respaldos diarios, semanales, mensuales, por año fiscal, por año natural y especiales. Se retendrá de forma permanente el

respaldo mensual, año fiscal y año natural. Todo respaldo producido para el final del mes y los producidos para fin de año (fiscal y natural) serán enviados a la bóveda.

**Efectos**

Las situaciones comentadas pueden ocasionar que, en casos de emergencias, la Administración no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones; y la pérdida permanente de información importante, sin la posibilidad de recuperarla.

**Causas**

La situación comentada se atribuye a que el Administrador del Centro de Información no realizó las gestiones necesarias para mantener las copias de los respaldos mensuales, y de los años fiscales y naturales en la bóveda externa.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos de Puerto Rico como medida de control interno y política de sana administración, compró el programa de resguardo […] y la librería de resguardo (tapes) […], con el propósito de realizar los resguardos diarios, semanales, mensuales, por año fiscal y natural, esto con el fin de conformar los cambios administrativos, operacionales y organizacionales de la agencia. Además, como parte del plan de acción correctiva de la Administración, se revisaron y actualizaron los procedimientos del proceso de resguardo contenidos en el Manual de Políticas y Procedimientos de la Oficina del Centro de Información. [*sic*]

**Véanse las recomendaciones 1 y 3.b.2).**

**Hallazgo 4 - Falta de revisiones periódicas de los registros de las transacciones críticas de la aplicación Sage ACCPAC y de seguridad provistos por el sistema operativo, y de los accesos a Internet**

**Situaciones**

a. La Administración tiene, como parte de sus programas computadorizados, una aplicación para procesar la información financiera de esta. La aplicación consistía de cuatro módulos

principales. Al 14 de junio de 2013, el registro de las transacciones críticas de esta aplicación se mantenía en un servidor. Dicho registro no se revisaba periódicamente con el propósito de controlar y garantizar la integridad, la exactitud y la validez de las transacciones de contabilidad de la Administración.

b. Al 2 de octubre de 2013, el Administrador del Centro de Información, quien era responsable de administrar la red y la seguridad de los sistemas computadorizados, no revisaba periódicamente los eventos o incidentes grabados en el registro *Security Log*[3] provistos por el sistema operativo del servidor configurado como *Primary Domain Controller (PDC)*. Esto era necesario para conocer las posibles violaciones de seguridad que pudieran ocurrir en los sistemas de información de la red y tomar prontamente las medidas preventivas y correctivas necesarias.

c. La Administración mantiene un servidor que permite el acceso a Internet a los usuarios autorizados. Al 19 de febrero de 2013, la Administración tenía 54 cuentas con los privilegios de acceder a Internet mediante dicho servidor. El servidor producía diariamente un archivo en el cual se registraban todas las páginas de direcciones de Internet *(web logs)* que fueron accedidas por las cuentas de los usuarios. Al 27 de noviembre de 2013, el Administrador del Centro de Información no verificaba periódicamente estos registros para examinar las páginas en Internet que acceden los usuarios autorizados.

**Criterios**

Las situaciones comentadas en los **apartados a. y b.** son contrarias a lo establecido en la *ATDI-106, Políticas de Seguridad y Mantenimiento en Áreas Críticas y Dispositivos de los Sistemas de Información*, del *Manual*. En esta se dispone, entre otras cosas, que se deben establecer controles para una efectiva disuasión y detección, a tiempo, de los intentos no

[3] El registro de la seguridad puede registrar acontecimientos de la seguridad, tales como tentativas válidas e inválidas de la conexión, y acontecimientos relacionados con el uso del recurso, como crear, abrir, o suprimir archivos. Un administrador puede especificar qué acontecimientos se registran en el registro de la seguridad.

autorizados para acceder a los sistemas y a los archivos de información. Además, son contrarias al *ATDI-304, Procedimiento de Monitoreo de los Sistemas de Información,* del *Manual*. En este se establecen los procedimientos a seguir para el monitoreo de los sistemas de información localizados en la Administración. También se indica que será responsabilidad del Administrador del Centro de Información monitorear la información generada por las distintas bitácoras de los servidores.

La situación comentada en el **apartado c.** se aparta de lo establecido en la *ATDI-100, Políticas de Uso y Manejo de Internet y de Correo Electrónico (E-MAIL),* del *Manual*. En esta se establece, entre otras cosas, que el oficial asignado para monitorear la seguridad y el buen funcionamiento de los muros protectores *(firewalls)* tendrá la responsabilidad de revisar y auditar los accesos para asegurar que se cumplan las políticas establecidas por la Administración. También es contraria a lo establecido en la *ATDI-104, Política de Acuerdo de Uso de Computadoras,* del *Manual*. En esta se establece, entre otras cosas, que la Administración puede rutinariamente generar un registro o monitorear directamente las comunicaciones de los empleados, por ejemplo, las páginas en Internet accedidas y la duración por página visitada, para los siguientes propósitos:

- Asignación de recursos
- Manejo óptimo de la información
- Detección de patrones que indiquen que un empleado está violando las políticas de la Administración o incurre en actividades ilegales.

**Efectos**

La situación comentada en el **apartado a.** puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas computadorizados sin que se puedan detectar a tiempo para fijar responsabilidades.

La situación comentada en el **apartado b.** propició que no se investigaran 38 eventos de seguridad grabados entre el 27 de septiembre y el 1 de octubre de 2013 en el *Security Log*, según se indica:

- Trece eventos *Logon failure*. *A logon attempt was made with an unknown user name or a known user name with a bad password (Event ID 529)*. Este evento se registra cuando un usuario intenta iniciar una sesión con una cuenta de usuario desconocido o con una cuenta de usuario válida del dominio, pero con una contraseña incorrecta.

- Dos eventos *Logon failure*. *The user attempted to log on with a password type that is not allowed (Event ID 534)*. Este evento indica que se hizo un intento para iniciar una sesión, pero la política de seguridad local del equipo no permite que el usuario inicie la sesión en la forma solicitada.

- Un evento *A disabled user account has been re-enabled (Event ID 626)*. Este evento indica que una cuenta de usuario desactivada ha sido reactivada. Pueden haber implicaciones de seguridad para esta acción.

- Cinco eventos *A user password was changed (Event ID 627)*. Este evento indica que se realizó un intento para cambiar la contraseña de la cuenta de un usuario de la red. En este mensaje se indica si el intento fue exitoso. La persona o el proceso para cambiar la contraseña tiene que proveer la contraseña anterior. Debido a que el usuario puede cambiar la contraseña sin iniciar sesión, el nombre del usuario *(Username)* puede ser mostrado como anónimo.

- Dos eventos *A user password was set (Event ID 628)*. Este evento indica que la contraseña de un usuario fue restablecida por otro usuario que tiene los privilegios para realizar dicho cambio. El usuario que restablece la contraseña no tiene que proporcionar la contraseña anterior.

- Cuatro eventos *A user account was changed (Event ID 642)*. Este evento indica que un atributo relevante a la seguridad de una cuenta de usuario fue cambiado. Este evento se genera sólo cuando uno de los atributos fue cambiado, tal como: Nombre asignado a la Cuenta, Parámetros del Usuario, Horas de Acceso y Última Contraseña Asignada.

- Un evento *A user account was automatically locked (Event ID 644)*. Este evento indica que una cuenta de usuario ha sido bloqueada. Una cuenta se bloquea cuando se produce un número específico de intentos fallidos de accesos a una sesión durante un período específico. Los intentos fallidos de acceso pueden indicar que el usuario olvidó la contraseña, que la contraseña está tratando de ser adivinada por un usuario no autorizado o algún tipo de ataque a la cuenta.

- Diez eventos *A set of credentials was passed to the authentication system on this computer either by a local process or by a remote process or user (Event ID 680).* Este evento indica que un conjunto de credenciales fueron transferidas al sistema de autenticación en la computadora, ya sea por un proceso local o por un proceso remoto.

Esto, a su vez, impidió la detección temprana de errores críticos o problemas con los servidores que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, privó a la gerencia de los medios necesarios para supervisar eficazmente el desempeño de los usuarios, y detectar el acceso y uso indebido de los sistemas computadorizados.

Lo comentado en el **apartado c.** impide la detección temprana del uso indebido del Internet, de manera que el Administrador del Centro de Información pueda tomar a tiempo las medidas correctivas o preventivas necesarias.

**Causas**

La situación comentada en el **apartado a.** se debía, en parte, a que la Directora de Presupuesto y Finanzas y el Administrador del Centro de Información no habían establecido una metodología para revisar el registro de las transacciones críticas de la aplicación financiera.

Lo comentado en el **apartado b.** se debía, en parte, a que el Administrador del Centro de Información, al ser el único empleado del Centro, realizaba todas las funciones relacionadas con los sistemas de información de la Administración. Por esto, se le hacía difícil la revisión periódica de los registros de seguridad y sólo los revisaba para documentar la investigación de situaciones irregulares.

La situación comentada en el **apartado c.** se debía, en parte, a que el servidor fue configurado para que el referido registro se produjera en un formato que el Administrador del Centro de Información no podía analizar, ya que no tenía disponibles las aplicaciones necesarias.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> El Administrador de la Oficina del Centro de Información de la Administración de Terrenos, emitirá reportes mensuales, "Event Viewer", donde se detallen los registros de las transacciones críticas de la aplicación […], de la seguridad provista por los sistemas operativos y de los accesos a Internet. Estos registros se revisaran y analizaran para tomar las medidas necesarias con el propósito de mejorar y/o mantener los controles internos adecuados, con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1 y 3 de la c. a la e.**

**Hallazgo 5 - Falta de documentación de la configuración de la red, deficiencias relacionadas con el diagrama esquemático de esta y con los controles físicos en las áreas de distribución de cableado**

**Situaciones**

a. Los equipos que componen la red de la Administración están distribuidos en dos pisos del edificio de esta. Cada piso cuenta con un

anaquel donde están ubicados los equipos de comunicaciones. El examen efectuado sobre la documentación de la red de la Administración reveló que:

1) El Centro de Información no mantenía la documentación de la configuración de la red, de los equipos conectados a esta ni de la distribución del cableado.

2) El diagrama esquemático de la infraestructura de la red de comunicaciones de la Administración suministrado para examen a nuestros auditores, no incluía la siguiente información importante:

- Las modificaciones realizadas en la composición de los servidores de la Administración
- El detalle de las computadoras y las impresoras conectadas a la red, con sus respectivas identificaciones y localizaciones
- El detalle de las conexiones del equipo y el cableado vertical *(backbone*[4]*)*
- La aprobación del Director Ejecutivo de la Administración.

b. El examen efectuado sobre los controles físicos en las áreas de distribución de cableado donde estaban instalados los equipos de comunicaciones de la Administración, reveló que los cables utilizados para las conexiones entre los equipos computadorizados y de comunicaciones (cableado) no estaban identificados. Esto era necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones.

**Criterio**

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 77-05*. En esta se establece que las agencias deben adquirir

[4] Línea de transmisión principal que transporta la información recopilada de líneas secundarias que están interconectadas a ellas.

e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. Además, incluye como política que el diseño de la red debe estar documentado.

Las mejores prácticas en el campo de la tecnología de información sugieren que para mantener en funciones aceptables la red es necesario establecer controles adecuados sobre los inventarios, la ubicación de los equipos y las conexiones entre sus componentes. Esto se logra mediante la documentación detallada y actualizada de las conexiones que permita corregir a tiempo problemas de comunicación de la red y detectar cualquier conexión no autorizada.

**Efectos**

Las situaciones comentadas impiden a la Administración tener una comprensión clara y precisa sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento a la misma. Además, dificulta atender problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

**Causas**

Las situaciones comentadas se atribuyen, en parte, a que el Administrador del Centro de Información no había tomado medidas de control para la identificación de los componentes y de la red, y la actualización de su documentación. Además, al implantar la nueva infraestructura de equipos de comunicación no se adquirió como parte de los servicios ofrecidos la identificación del cableado y la preparación de la documentación de la configuración de la red, de los equipos conectados a esta y de los diagramas esquemáticos.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos, una vez recibido el 1er Borrador de los Hallazgos en Marzo 2014, contrato a la compañía […] para que asistiera al

> Administrador del Centro de Información de la agencia, a la instalación y certificación del cableado y de la infraestructura de la red de la Administración, esto con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1 y 3 de la f. a la h.**

**Hallazgo 6 - Deficiencias relacionadas con los procedimientos escritos para la disposición de la información sensitiva almacenada y de los programas instalados en las computadoras de la Administración**

**Situación**

a. Al 15 de noviembre de 2013, la Administración tenía el *ATDI-204, Procedimiento para Disposición de Computadoras y Dispositivos*, del *Manual*. En este se establecían los controles de la Administración para la disposición, la transferencia, la donación y el reciclaje de todos los componentes del equipo electrónico que haya sido declarado inservible. El examen realizado al 15 de noviembre de 2013, sobre el contenido del *Procedimiento ATDI-204*, reveló que en el mismo no se contempla un proceso para controlar eficazmente la disposición de la información sensitiva y de los programas antes de transferir o disponer de los equipos computadorizados.

**Criterios**

La situación comentada es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que cuando las entidades gubernamentales vayan a disponer de equipo que contiene información sensitiva deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las instalaciones de la agencia.

Además, se aparta de lo establecido en la *Política TIG-007, Disposición de Equipo y Licencias*, de dicha *Carta Circular*. En esta se establecen los mecanismos que las entidades gubernamentales implantarán para asegurarse de que se disponga apropiadamente del equipo de tecnologías de información, así como de los programas que tuviesen los mismos instalados, si alguno.

**Efectos**

La situación comentada puede propiciar que, al momento de transferir o disponer de los equipos computadorizados, no se considere la eliminación de la información confidencial y de los programas almacenados en los mismos. Esto, a su vez, puede propiciar que personas no autorizadas puedan lograr acceso a información confidencial y que la misma sea divulgada o utilizada indebidamente. Además, podría ocasionar situaciones que afecten los derechos de terceros, por los cuales se responsabilice a la Administración.

**Causa**

La situación comentada se atribuye, en parte, a que el Administrador del Centro de Información no había considerado modificar el *Procedimiento ATDI-204* para que incluyera el proceso para la disposición de la información sensitiva mantenida en los discos duros de las computadoras y los programas instalados en estas.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos, una vez recibido el 1er Borrador de los Hallazgos en Marzo 2014, contrato a la compañía […] (consultores) para que revisara y actualizara el "Manual de Políticas y Procedimientos del Centro de Información". También se contrataron sus servicios para desarrollar e implementar políticas nuevas, necesarias y requeridas para mantener un mejor control del uso y contenido de los sistemas computadorizados de la Administración, esto con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1 y 3.i.**

**Hallazgo 7 - Falta de actualización y de cumplimiento de los procedimientos, y formularios sin utilizar**

**Situaciones**

a. En el *Manual* se establecen las guías, las políticas y los procedimientos para asegurar que las ejecutorias del Centro de Información se efectúen y completen de acuerdo con los estándares

establecidos por la Administración. El examen realizado entre el 27 de noviembre de 2013 y el 19 de febrero de 2014 sobre el cumplimiento del Centro de Información con las políticas y los procedimientos del *Manual* reveló que:

1) El *Manual* no había sido revisado ni actualizado desde su aprobación el 28 de abril de 2005 para incorporar, entre otras cosas, los cambios en la configuración y los componentes de la red.

2) No se habían realizado auditorías, por parte del Administrador del Centro de Información, para verificar la condición de los equipos en intervalos menores de tres años.

3) El Administrador del Centro de Información no había realizado auditorías para verificar el cumplimiento en el uso de las licencias de aplicaciones, herramientas y programas.

4) No se efectuaban revisiones periódicas de las autorizaciones de acceso físico al Centro de Información.

5) No se utilizaba el formulario *Solicitud para la Remoción de Usuario (ATDI- 903)*. Este se debía completar para evidenciar el proceso de solicitud de eliminación de las cuentas de acceso al sistema cuando un empleado es removido de su puesto permanente o temporalmente.

6) No se preparaba anualmente el *Plan Estratégico de Informática* o *Plan de Mecanización*.

**Criterios**

La situación comentada en el **apartado a.1)** es contraria a lo establecido en el *ATDI-400, Procedimiento de Mantenimiento del Manual de Políticas y Procedimientos*, del *Manual*. En este se establece que se realizará una revisión mandatoria de toda la documentación contenida en el *Manual* una vez al año. Dicha revisión será responsabilidad del Comité Evaluador[5].

[5] El Comité está compuesto por el Subdirector Ejecutivo; los directores de Presupuesto y Finanzas, de Recursos Humanos y de Servicios Generales; el Auditor Interno y el Administrador del Centro de Información.

Este verificará todo el *Manual* para identificar los cambios que hayan surgido como consecuencia de nuevas políticas, tecnologías, leyes y reglamentos, entre otros. Una vez el *Manual* haya sido recomendado por el Comité Evaluador se remite para la aprobación final del Director Ejecutivo y de la Junta de Gobierno.

Lo comentado en el **apartado a.2)** es contrario a lo establecido en la *ATDI-101, Política de Adquisición de Equipo Físico y/o Dispositivos,* del *Manual*. En esta se establece, entre otras cosas, que el Administrador del Centro de Información efectuará auditorías para verificar la condición del equipo de cada uno de los usuarios. Dicha auditoría no debe exceder el término de tres años, que es la cantidad máxima de garantía ofrecida por los manufactureros.

La situación comentada en el **apartado a.3)** es contraria a lo establecido en la *ATDI-102, Políticas de Aplicaciones, Herramientas y Programas,* del *Manual*. En estas se establece que el Administrador del Centro de Información realizará auditorías al azar de todas las computadoras de la Administración para asegurar de que se esté cumpliendo con todas las licencias de aplicaciones, herramientas y programas. Dichas auditorías serán realizadas, por lo menos, una vez al año o según el criterio del Administrador del Centro de Información.

Lo comentado en el **apartado a.4)** es contrario a lo establecido en la *ATDI-106, Política de Seguridad y Mantenimiento en Áreas Críticas y Dispositivos de los Sistemas de Información,* del *Manual*. En esta se indica que se deben establecer políticas de autorizaciones de acceso físico al Centro de Información y revisiones periódicas de dichas autorizaciones.

La situación comentada en el **apartado a.5)** es contraria a lo establecido en el *ATDI-301, Procedimiento para la Remoción de Usuarios,* del *Manual*. En este se indica que el Técnico de Recursos Humanos y Relaciones Laborales completará el *Formulario ATDI-903* cada vez que un empleado sea removido de su puesto y se lo enviará por correo electrónico o entregará a la mano al Administrador del Centro de Información, para que realice las modificaciones pertinentes.

Lo comentado en el **apartado a.6)** es contrario a lo establecido en el *ATDI-206, Plan Estratégico del Departamento de Informática*, del *Manual*. En este se establece que el Administrador del Centro de Información preparará el *Plan de Mecanización* con los requerimientos de cada una de las oficinas. El *Plan de Mecanización* se generará y se evaluará anualmente cuando se esté preparando el presupuesto de la agencia para el próximo período fiscal.

**Efectos**

Las situaciones comentadas pueden ocasionar que:

- Los mecanismos de control y las operaciones de la Administración y del Centro de Información no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias. Además, esto podría reducir la efectividad de los sistemas computadorizados; expondría al personal del Centro de Información, a los equipos y a la información a riesgos innecesarios; y afectaría la continuidad de las operaciones. **[Apartado a.1)]**

- Exista equipo dañado y venza su garantía sin tomar acción al respecto. También pudiera generar que exista equipo hurtado o perdido y la situación no sea detectada. **[Apartado a.2)]**

- Proliferación de programas o aplicaciones ilegales instalados en los sistemas de la Administración, lo que podría generar multas para la Administración. **[Apartado a.3)]**

- Personas ajenas a la Administración tengan acceso al equipo computadorizado y a la información que reside en este, y puedan dañar, destruir o comprometer la seguridad e integridad de la misma. **[Apartado a.4)]**

- Se mantengan activas las cuentas de acceso a los sistemas de información de la Administración correspondientes a exempleados, luego de su separación. Al 22 de octubre de 2013, esto ocurrió con las

cuentas de acceso correspondientes a cinco exempleados que cesaron sus funciones entre el 30 de junio y el 18 de octubre de 2013. **[Apartado a.5)]**

- No se destinen los recursos presupuestarios necesarios para cubrir las necesidades relacionadas con los sistemas de información y el logro de las metas establecidas. **[Apartado a.6)]**

**Causas**

Las situaciones comentadas se atribuyen, en parte, a que el Administrador del Centro de Información se había apartado de las políticas y de los procedimientos establecidos en el *Manual*; a la falta de personal en el Centro de Información; y a la falta de supervisión de las funciones realizadas por este de parte del Director Ejecutivo.

**Comentarios de la Gerencia**

En la carta del Director Ejecutivo, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina del Centro de Información de la Administración de Terrenos, una vez recibido el 1er Borrador de los Hallazgos en Marzo 2014, contrato a la compañía […] (consultores) para que revisara y actualizara el "Manual de Políticas y Procedimientos del Centro de Información". También se contrataron sus servicios para desarrollar e implementar políticas nuevas, necesarias y requeridas para mantener un mejor control del uso y contenido de los sistemas computadorizados de la Administración, esto con el fin de cumplir con la política de sana administración y como parte del plan de acción correctiva de la agencia. [*sic*]

**Véanse las recomendaciones 1, 3 de la j. a la n. y 5.**

## RECOMENDACIONES

**Al Presidente de la Junta de Gobierno de la Administración de Terrenos de Puerto Rico**

1. Ver que el Director Ejecutivo de la Administración cumpla con las **recomendaciones de la 2 a la 5** de este *Informe*. **[Hallazgos del 1 al 7]**

**Al Director Ejecutivo de la Administración de Terrenos de Puerto Rico**

2. Asegurarse de que se realicen y se documenten los análisis de riesgos de los sistemas de información computadorizados y de impacto de negocios, según se establece en el *ATDI-600* y en las políticas *TIG-003* y *TIG-015* de la *Carta Circular 77-05*; y que los mismos sean remitidos para su revisión y aprobación. **[Hallazgo 1]**

3. Ejercer una supervisión efectiva sobre el Administrador del Centro de Información para asegurarse de que:

    a. Prepare y remita para su aprobación:

        1) Un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de operaciones, según se establece en las políticas *TIG-003*, *TIG-004* y *TIG-015*. Una vez el *Plan* sea revisado y aprobado, asegurarse de que se realicen pruebas periódicas y se divulgue a los empleados y a los funcionarios concernientes. Además, se mantenga una copia del mismo en un lugar seguro fuera de los predios de la Administración. **[Hallazgo 2-a.]**

        2) Un *Plan de Contingencias* que incluya los aspectos comentados en el **Hallazgo 2-b.** y lo remita para su aprobación.

    b. Realice las gestiones necesarias para:

        1) Identificar un centro alterno que acepte la utilización de sus equipos en caso de desastres o emergencias en la Administración, o para que se establezca un centro alterno propio en alguna instalación que no esté expuesta a los mismos riesgos que el lugar donde se encuentra el Centro de Información. **[Hallazgo 2-c.]**

        2) Obtener los medios de almacenaje suficientes para efectuar los respaldos mensuales y anuales (fiscal y natural) de la información almacenada en los servidores de la

Administración, y los almacene y retenga en la bóveda externa según se dispone en el *Procedimiento ATDI-401*. **[Hallazgo 3]**

c. En coordinación con la Directora de Presupuesto y Finanzas, establezca una metodología para efectuar revisiones periódicas de las transacciones críticas de la aplicación financiera. **[Hallazgo 4-a.]**

d. Efectúe revisiones periódicas de los eventos o incidentes grabados en el *Security Log* provisto por el sistema operativo del servidor configurado como *PDC* y documente en un registro las revisiones e investigaciones efectuadas. **[Hallazgo 4-b.]**

e. Identifique y adquiera una aplicación para analizar los registros de direcciones en Internet visitadas por los usuarios y registradas en el servidor que provee dicho servicio. Además, que se adiestre sobre la utilización de la misma para así revisar periódicamente dichos registros. **[Hallazgo 4-c.]**

f. Realice las gestiones necesarias para que se prepare la documentación de la configuración de la red, de los equipos conectados a esta y de la distribución del cableado. **[Hallazgo 5-a.1)]**

g. Actualice el diagrama esquemático de la red de la Administración, dentro de un término razonable, para que incluya la información descrita en el **Hallazgo 5-a.2)**. Una vez se actualice, mantener copia del diagrama esquemático del cableado en un espacio visible en las áreas de distribución.

h. Identifique los cables de las áreas de distribución de cableado, de manera que se pueda determinar con facilidad a qué computadora pertenecen y corregir a tiempo los problemas de comunicación. **[Hallazgo 5-b.]**

i. Revise y remita para la consideración del Comité Evaluador el *Procedimiento ATDI-204* del *Manual* para que incluya el proceso para la eliminación de la información sensitiva mantenida en los discos duros de las computadoras y los programas instalados en estas antes de transferir, donar o disponer las mismas. Una vez el Comité Evaluador recomiende las modificaciones al procedimiento, lo remita al Director Ejecutivo para aprobación. **[Hallazgo 6]**

j. Revise anualmente el *Manual* para identificar aquellos cambios que hayan surgido e incorpore dichos cambios, y los envíe para la verificación y recomendación del Comité Evaluador. Si este Comité está de acuerdo con los cambios efectuados, envíe el mismo al Director Ejecutivo para aprobación final. **[Hallazgo 7-a.1)]**

k. Efectúe auditorías para verificar:

1) La condición del equipo en intervalos menores de tres años. **[Hallazgo 7-a.2)]**

2) El cumplimiento en el uso de todas las licencias de aplicaciones, herramientas y programas. **[Hallazgo 7-a.3)]**

l. Efectúe revisiones periódicas de las autorizaciones de acceso físico al Centro de Información. **[Hallazgo 7-a.4)]**

m. Vele por que se complete el *Formulario ATDI-903* para toda solicitud de eliminación de una cuenta de acceso al sistema. **[Hallazgo 7-a.5)]**

n. Prepare y mantenga actualizado en una base anual el *Plan Estratégico* o *Plan de Mecanización* del Centro de Informática, y lo remita al Director Ejecutivo y al Director de Presupuesto y Finanzas para verificación y comentarios. **[Hallazgo 7-a.6)]**

4. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus respectivos equipos en caso de desastres o emergencias en la Administración. **[Hallazgo 2-c.]**

5. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos y Relaciones Laborales para que se asegure de que cada vez que un empleado sea removido de su puesto, ya sea permanente o temporeramente, el Técnico de Recursos Humanos y Relaciones Laborales complete el *Formulario ATDI-903*, y lo envíe al Administrador del Centro de Información por correo electrónico o lo entregue a la mano con, por lo menos, dos semanas de antelación, en los casos que sea posible. **[Hallazgo 7-a.5)]**

**AGRADECIMIENTO**

A los funcionarios y a los empleados de la Administración de Terrenos de Puerto Rico, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor

Por:

**ANEJO 1**

ADMINISTRACIÓN DE TERRENOS DE PUERTO RICO
CENTRO DE INFORMACIÓN
**MIEMBROS PRINCIPALES DE LA JUNTA DE GOBIERNO**
**DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Hon. Alberto Bacó Bagué | Presidente | 18 feb. 13 | 19 feb. 14 |
| Plan. Luis García Pelatti | Vicepresidente | 18 feb. 13 | 19 feb. 14 |
| Ing. Antonio L. Medina Comas | Miembro | 18 feb. 13 | 19 feb. 14 |
| Hon. Rubén Ríos Pagán | " | 18 feb. 13 | 19 feb. 14 |
| Hon. Melba Acosta Febo | " | 18 feb. 13 | 19 feb. 14 |
| Hon. Miguel A. Torres Díaz | " | 18 feb. 13 | 19 feb. 14 |
| Hon. Myrna Comas Pagán | " | 28 dic. 13 | 19 feb. 14 |
| Sr. Carlos López Lay | Miembro del Sector Privado | 27 sep. 13 | 19 feb. 14 |

**ANEJO 2**

ADMINISTRACIÓN DE TERRENOS DE PUERTO RICO
CENTRO DE INFORMACIÓN
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD**
**DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Agro. Luis Rivero Cubano | Director Ejecutivo | 16 ago. 13 | 19 feb. 14 |
| Arq. Carlos I. Mejía Algarín | Director Ejecutivo Interino | 1 jul. 13 | 15 ago. 13 |
| Sra. María de L. Blázquez Arsuaga | Directora Ejecutiva | 18 feb. 13 | 30 jun. 13 |
| Arq. Carlos I. Mejía Algarín | Subdirector Ejecutivo | 18 feb. 13 | 19 feb. 14 |
| Sr. Mario Hiraldo Ventura | Administrador del Centro de Información | 18 feb. 13 | 19 feb. 14 |
| CPA Nurys Paniagua Charles | Directora de Presupuesto y Finanzas | 19 ene. 14 | 19 feb. 14 |
| " | Directora de Presupuesto y Finanzas Interina | 18 feb. 13 | 16 ene. 14 |
| Sra. Joanne M. López Corsino | Directora de Recursos Humanos y Relaciones Laborales | 16 oct. 13 | 19 feb. 14 |
| Lcdo. Frank Pérez Jiménez | Director Interino de Recursos Humanos y Relaciones Laborales | 1 oct. 13 | 15 oct. 13 |
| Sra. Ivonne Martínez Burgos | Directora de Recursos Humanos y Relaciones Laborales | 18 feb. 13 | 30 sep. 13 |

**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 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