

INFORME DE AUDITORÍA TI-10-11

3 de febrero de 2010

Autoridad de Desperdicios Sólidos en Puerto Rico

Oficina de Sistemas de Información

(Unidad 5006 - Auditoría 13016)

Período auditado: 1 de junio de 2007 al 30 de abril de 2008

CONTENIDO

	Página
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	3
RESPONSABILIDAD DE LA GERENCIA	5
ALCANCE Y METODOLOGÍA	6
OPINIÓN	6
RECOMENDACIONES	6
AL SECRETARIO DE RECURSOS NATURALES Y AMBIENTALES	6
A LA DIRECTORA EJECUTIVA DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO	7
CARTAS A LA GERENCIA	10
COMENTARIOS DE LA GERENCIA	10
AGRADECIMIENTO	11
RELACIÓN DETALLADA DE HALLAZGOS	12
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO	12
HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO.....	13
1 - Utilización de computadoras e instalación de programas no autorizados para fines ajenos a la gestión pública, y falta de controles para prevenir y detectar la instalación de programas no autorizados y la remoción de programas instalados	13
2 - Falta de controles relacionados con los equipos computadorizados	18
3 - Normas y procedimientos importantes no incluidos en la reglamentación aprobada para la seguridad y el uso de los sistemas de información computadorizados, y falta de normas y de procedimientos escritos para la instalación y la configuración de la red	22
4 - Deficiencia relacionada con la Certificación de Recibo, Aceptación y Conocimiento de Medidas Disciplinarias, y faltas de control de la misma.....	25

5 - Deficiencias en los cuartos de distribución del cableado (<i>wiring closets</i>) de la red y en el área de los servidores del Centro de Cómputos	27
6 - Falta de adiestramientos periódicos al Administrador de la Red de la Autoridad	30
7 - Deficiencias relacionadas con la documentación de la configuración de las instalaciones de la red	31
ANEJO - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO	34

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

3 de febrero de 2010

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Autoridad de Desperdicios Sólidos en Puerto Rico (Autoridad) para determinar si se hicieron 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. Efectuamos la misma a base de la facultad que 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.

Determinamos emitir dos informes de esta auditoría. Este es el último informe y contiene el resultado de nuestro examen de los controles internos establecidos para el uso de las computadoras, la red de comunicaciones (red) e Internet. El primer informe se emitió el 21 de octubre de 2009 y contiene el resultado de nuestro examen de los controles internos relacionados con el acceso lógico a los sistemas de información computadorizados, la administración del programa de seguridad, la segregación de deberes y la evaluación de la continuidad del servicio establecidos en la OSI (*Informe de Auditoría TI-10-07*).

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Autoridad se creó mediante la *Ley Núm. 70 del 23 de junio de 1978*, según enmendada, para planificar, financiar y operar los servicios de trasbordo, procesamiento, recuperación y disposición final de los desperdicios sólidos por agencias de recolección públicas y privadas de Puerto Rico. En ésta se dispone que será política pública del

Estado Libre Asociado de Puerto Rico desarrollar e implantar estrategias económicamente viables y ambientalmente seguras que redunden en la reducción de residuos sólidos, a la vez que estimulen la participación de entidades privadas en la construcción y la operación de instalaciones de recuperación y reciclaje.

Mediante el Artículo 6 del *Plan de Reorganización Núm. 1 de 1993*, aprobado por la Asamblea Legislativa de Puerto Rico, el cual creó el Departamento de Recursos Naturales y Ambientales (Departamento), se suprimió la Junta de Gobierno de la Autoridad y las facultades de ésta se transfirieron al Secretario de Recursos Naturales y Ambientales (Secretario). Entre dichas facultades, están las de adoptar normas y establecer la política pública de la Autoridad. Además, se creó la Junta Asesora de Desperdicios Sólidos, adscrita a la Autoridad. Las funciones ejecutivas de la Autoridad las ejerce un Director Ejecutivo nombrado por el Secretario.

El Director Ejecutivo de la Autoridad cuenta, para el desempeño de sus funciones, con las siguientes unidades de asesoramiento que le responden directamente: División de Planificación, Área de Operaciones e Ingeniería, Oficina de Desarrollo de Mercados, Oficina de Educación y Reciclaje, División Legal, División de Asuntos Gerenciales, Oficina de Recursos Humanos, y Oficina de Secretaría. La OSI responde al Director de Asuntos Gerenciales. La estructura organizacional de la OSI consiste de un Oficial Principal de Informática¹, un Gerente de Sistemas de Información y dos analistas programadores.

El **ANEJO** contiene una relación de los funcionarios principales de la Autoridad que actuaron durante el período auditado.

Los gastos operacionales de la OSI se sufragan del presupuesto operacional de la Autoridad que para el año fiscal 2006-07 ascendió a \$5,884,000.

¹ A la fecha de la auditoría este puesto estaba vacante.

Al 30 de abril de 2008, estaban pendientes de resolución por los tribunales cinco demandas civiles presentadas contra la Autoridad por \$25,032,738. De este importe, \$14,000,000 eran por daños y perjuicios, \$950,000 por arbitraje, y \$10,082,738 por cobro de dinero.

La Autoridad tiene una red con 7 servidores mediante los cuales se procesan 11 aplicaciones. También cuenta con una página en Internet a la cual se puede acceder mediante la siguiente dirección: <http://www.ads.gobierno.pr>. Esta página provee información acerca de la entidad y de los servicios que presta.

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes *Diez Principios para Lograr una Administración Pública de Excelencia*. Éstos se rigen por principios de calidad y por los valores institucionales:

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.
2. Mantener una oficina de auditoría interna competente.
3. Cumplir con los requisitos impuestos por las agencias reguladoras.
4. Adoptar un plan estratégico para las operaciones.
5. Mantener el control presupuestario.
6. Mantenerse al día con los avances tecnológicos.
7. Mantener sistemas adecuados de archivo y de control de documentos.
8. Cumplir con el *Plan de Acción Correctiva* de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.
9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.
10. Cumplir con la *Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, lo cual incluye divulgar sus disposiciones a todo el personal.

El 27 de junio de 2008, mediante la *Carta Circular OC-08-32*, divulgamos la revisión de los mencionados diez principios, establecidos en nuestra *Carta Circular OC-98-09* del 14 de abril de 1998. Se puede acceder a ambas cartas circulares a través de nuestra página en Internet: <http://www.ocpr.gov.pr>.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de junio de 2007 al 30 de abril de 2008. En algunos aspectos examinamos operaciones 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.

Para efectuar la auditoría utilizamos la siguiente metodología:

- entrevistas a funcionarios, a empleados y a particulares
- inspecciones físicas
- examen y análisis de informes y de documentos generados por la unidad auditada
- examen y análisis de informes y de documentos suministrados por fuentes externas
- pruebas y análisis de procedimientos de control interno y de otros procesos.

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI, en lo que concierne a los controles establecidos para las computadoras, la red e Internet, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 7**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

RECOMENDACIONES

AL SECRETARIO DE RECURSOS NATURALES Y AMBIENTALES

1. Ver que la Directora Ejecutiva de la Autoridad cumpla con las **recomendaciones de la 3 a la 9** de este *Informe*. [**Hallazgos del 1 al 7**]

2. Ver que la Directora Ejecutiva de la Autoridad revise y actualice la *Carta Circular Núm. 2003-01, Para Establecer la Política de la Autoridad de Desperdicios Sólidos en Cuanto al Uso, Manejo y Conservación de Computadoras; el Uso y Manejo Adecuado del Internet y el Uso y Manejo Adecuado del Correo Electrónico*, aprobada el 9 de mayo de 2003 por el Director Ejecutivo de la Autoridad, conforme a las normas y a los procedimientos sugeridos en el **Hallazgo 3-a.**, y la remita para su consideración y aprobación. Una vez aprobada, se asegure de que sea de conocimiento de todo el personal que utiliza los sistemas de información de la Autoridad.

A LA DIRECTORA EJECUTIVA DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO

3. Ejercer una supervisión efectiva sobre el Gerente de Sistemas de Información de la OSI para asegurarse de que:
 - a. Oriente a los funcionarios y a los empleados de la Autoridad sobre el uso adecuado, las restricciones y el manejo correcto de las computadoras y de las cuentas para acceder a Internet y al correo electrónico, y conserve evidencia de dicha orientación. **[Hallazgo del 1-a.1) al 4)]**
 - b. Establezca por escrito los controles necesarios para asegurarse de que los sistemas computadorizados se utilizan para asuntos oficiales; y para la detección y la corrección de virus o programas no deseados. Además, vea que se cumpla con dichos controles. **[Hallazgo del 1-a.1) al 5)]**
 - c. Realice inspecciones periódicas para asegurarse de que los usuarios cumplan con las normas establecidas sobre el uso de las computadoras y de las cuentas para acceder a Internet y al correo electrónico. **[Hallazgo del 1-a.1) al 4)]**
 - d. Realice las gestiones pertinentes para que se instalen programas antivirus en todas las computadoras de la Autoridad. **[Hallazgo 1-a.5)]**

- e. Establezca los controles necesarios para restringir el acceso de los usuarios de las computadoras a la opción *Add/Remove Programs* del sistema operativo. Esto, para que los usuarios no puedan instalar o remover programas. **[Hallazgo 1-a.4) y 6)]**
 - f. Redacte las normas y los procedimientos necesarios para la instalación y la configuración de la red, y los remita para la consideración y la aprobación del Secretario. **[Hallazgo 3-b.]**
 - g. Realice las gestiones que correspondan para que:
 - 1) La compañía a cargo de la infraestructura de la red prepare un diagrama de los *drops* e incluya copia de éste en un área visible en los cuartos de distribución del cableado. **[Hallazgo 5-a.1)]**
 - 2) Se provea servicio de mantenimiento a los cuartos de distribución de cableado de la red para que se cumpla con las condiciones ambientales, y se evite mantener en los mismos los materiales indicados en el **Hallazgo 5-a.2).**
 - 3) Se instalen generadores de energía ininterrumpible a los equipos de comunicaciones de la red. **[Hallazgo 5-a.3)]**
 - h. Requiera a la compañía consultora contratada que actualice el diagrama de la red para que se incluya la información descrita en el **Hallazgo 7.**
 - i. Documente la instalación y la configuración del sistema operativo de cada computador principal, de las aplicaciones utilizadas en la Autoridad y del equipo de comunicación conectado a la red. **[Hallazgo 7]**
4. Ver que el Director de Asuntos Fiscales ejerza una supervisión eficaz sobre las funciones del Director Interino de Servicios Generales para asegurarse de que el Encargado de la Propiedad:
- a. Actualice el inventario de la propiedad conforme a la ubicación física de las computadoras. **[Hallazgo 2-a.]**

- b. Tome las medidas necesarias para que se cumpla con las disposiciones relacionadas con la administración y el control de la propiedad, de manera que no se repita la situación comentada en el **Hallazgo 2-c.**
5. Ejercer una supervisión eficaz sobre los supervisores de los empleados para asegurarse de que cumplan con las disposiciones establecidas en el *Reglamento de Uso, Control y Disposición de Propiedad Mueble*, según enmendado, promulgado el 17 de diciembre de 1992 por el Director Ejecutivo de la Autoridad y el Presidente de la Junta de Gobierno². [**Hallazgo 2-a.**]
6. Determinar de quién será la responsabilidad de los equipos ubicados en los cuartos de cableado del Edificio de Agencias Ambientales, de manera que el Funcionario Administrativo I quien funge como Encargado de la Propiedad pueda asignarle un número de propiedad, e identificarlo y registrarlo en el sistema computadorizado de propiedad de la Autoridad. [**Hallazgo 2-b.**]
7. Enmendar el formulario *Certificación de Recibo* para que requiera la firma del supervisor del empleado como evidencia de haber suministrado a éste la *Carta Circular Núm. 2003-01*. [**Hallazgo 4-a.**]
8. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para que se asegure de que la *Carta Circular Núm. 2003-01* se le entregue a cada empleado de la Autoridad y se conserve copia de la *Certificación de Recibo, Aceptación y Conocimiento de Medidas Disciplinarias* en los expedientes de éstos. [**Hallazgo 4-b.**]
9. Asignar los recursos económicos necesarios a la OSI para que el Gerente de Sistemas de Información de la OSI establezca e implante un programa de adiestramiento continuo para el Administrador de la Red. [**Hallazgo 6**]

² Mediante el *Plan de Reorganización Núm. 1 de 1993* se suprimió la Junta de Gobierno de la Autoridad.

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este *Informe* se remitió al Hon. Daniel J. Galán Kercadó, Secretario de Recursos Naturales y Ambientales, y al Lcdo. Luis M. Bernal Jiménez, Director Ejecutivo de la Autoridad, para comentarios, en cartas del 8 de septiembre de 2009. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Sr. Javier Vélez Arocho, ex Secretario de Recursos Naturales y Ambientales, y al Dr. Javier A. Quintana Méndez, ex Director Ejecutivo de la Autoridad, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por la Autoridad.

COMENTARIOS DE LA GERENCIA

El 22 de septiembre de 2009, el Director Ejecutivo solicitó una prórroga de 15 días para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 24 de septiembre de 2009, le concedimos al Director Ejecutivo la prórroga hasta el 8 de octubre de 2009. El 8 de octubre de 2009, el Sr. Antonio Ríos Díaz, Director Ejecutivo Interino, solicitó una nueva prórroga. El 9 de octubre de 2009, le concedimos la prórroga solicitada hasta el 16 de octubre de 2009. La Ing. Rebeca Nieves, Directora Ejecutiva de la Autoridad, contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 23 de octubre de 2009. Sus comentarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la sección de la segunda parte de este *Informe*, titulada HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO.

El Secretario de Recursos Naturales y Ambientales contestó el borrador de los **hallazgos** de este *Informe* en carta del 21 de septiembre de 2009. En dicha carta informó que los comentarios los incluirá en los planes de acción correctiva que remitirá para adoptar las recomendaciones.

El ex Secretario de Recursos Naturales y Ambientales y el ex Director Ejecutivo de la Autoridad no contestaron el borrador de los **hallazgos** de este *Informe* que les fuera remitido para comentarios en nuestras cartas del 8 de septiembre de 2009, y en cartas de seguimiento del 25 de septiembre de 2009.

AGRADECIMIENTO

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

Por: *Yolanda del Cordero*
Interventora Jy C

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas. Éstos se clasifican como principales o secundarios. Los principales incluyen desviaciones de disposiciones sobre las operaciones de la unidad auditada que tienen un efecto material, tanto en el aspecto cuantitativo como en el cualitativo. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves.

Los hallazgos del informe se presentan según los atributos establecidos conforme a las normas de redacción de informes de nuestra Oficina. El propósito es facilitar al lector una mejor comprensión de la información ofrecida. Cada uno de ellos consta de las siguientes partes:

Situación - Los hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.

Criterio - El marco de referencia para evaluar la situación. Es principalmente una ley, un reglamento, una carta circular, un memorando, un procedimiento, una norma de control interno, una norma de sana administración, un principio de contabilidad generalmente aceptado, una opinión de un experto o un juicio del auditor.

Efecto - Lo que significa, real o potencialmente, no cumplir con el criterio.

Causa - La razón fundamental por la cual ocurrió la situación.

Al final de cada hallazgo se hace referencia a las recomendaciones que se incluyen en el informe para que se tomen las medidas necesarias sobre los errores, las irregularidades o los actos ilegales señalados.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los ex funcionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se

consideran al revisar el borrador del informe; y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO, de forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, éste prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO

Los **hallazgos** de este *Informe* se clasifican como principales.

Hallazgo 1 - Utilización de computadoras e instalación de programas no autorizados para fines ajenos a la gestión pública, y falta de controles para prevenir y detectar la instalación de programas no autorizados y la remoción de programas instalados

a. El *Asset Listing Report*³ de la Autoridad del 7 de noviembre de 2007, el cual nos proveyó el Funcionario Administrativo I quien funge como Encargado de la Propiedad, contenía 225 computadoras adquiridas por \$290,820. De éstas, 59 fueron donadas por el Departamento y tenían un valor asignado de \$1 por computadora. Las computadoras estaban localizadas en la Oficina Central de la Autoridad. El examen del uso de 15 computadoras, realizado del 11 de diciembre de 2007 al 12 de febrero de 2008, reveló las siguientes irregularidades:

- 1) Una computadora⁴ (7 por ciento), localizada en la Oficina de Reciclaje y Educación, contenía documentos ajenos a la gestión pública.

³ Informe que contiene la propiedad mueble de la Autoridad.

⁴ Una relación de las computadoras se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al ex Secretario de Recursos Naturales y Ambientales, y al Director Ejecutivo y al ex Director Ejecutivo de la Autoridad.

- 2) Seis computadoras⁵ (40 por ciento) se utilizaron para examinar páginas en Internet cuyo contenido era ajeno a la gestión pública.
- 3) Nueve computadoras⁵ (60 por ciento) se utilizaron para enviar o recibir mensajes de correo electrónico cuyo contenido era ajeno a la gestión pública.
- 4) Dos computadoras⁵ (13 por ciento) tenían instalados programas no autorizados y de libre distribución (*freeware*) que no guardaban relación con los trabajos que se realizaban en la Autoridad.
- 5) Tres computadoras⁵ (20 por ciento) no tenían instalado un programa antivirus.
- 6) Quince computadoras⁵ no tenían controles para impedir el acceso a la opción *Add/Remove Programs* del sistema operativo. Esto, para imposibilitar que los usuarios instalen programas no autorizados o remuevan programas autorizados. El acceso a dicha opción solamente debe estar disponible para el Encargado del Sistema.

En el Artículo VI, Sección 9 de la Constitución se establece que: “Sólo se dispondrá de las propiedades y fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado, y en todo caso por autoridad de ley”. [*sic*]

En el Artículo 3.2(c) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, según enmendada, se dispone, entre otras cosas, que ningún funcionario o empleado público utilizará propiedad pública para obtener directa o indirectamente ventajas, beneficios o privilegios que no estén permitidos por ley.

⁵ Véase la nota al calce 4.

En la *Carta Circular Núm. 2003-01* se establece lo siguiente:

Los sistemas de comunicación y acceso a Internet son propiedad de la Autoridad, se ofrecerán a los usuarios como herramienta de trabajo en el desempeño de sus funciones. Se prohíbe terminantemente el uso de los sistemas de computadoras y comunicaciones de la Autoridad para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena o envío de mensajes sin contenido oficial. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la Autoridad para obtener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno al desempeño de sus funciones en la Agencia.

La información contenida en las computadoras, sistemas, correspondencia electrónica, documentos, programas y servicios asociados, tanto internos como externos, no podrán reproducirse, o utilizarse de manera alguna para fines ajenos a las funciones de la Autoridad.

Queda expresamente prohibido utilizar el correo electrónico para enviar mensajes que puedan considerarse irresponsables, molestosos, hostigantes, u ofensivos, incluyendo pero no ilimitados a comentarios o imágenes de contenido sexual, racial y utilizar lenguaje descortés.

Se prohíbe terminantemente copiar programas protegidos por las leyes de derecho de autor o tener instalados programas sin licencias. La Autoridad no requiere, solicita ni condona la duplicación o uso no autorizado de programas protegidos por derechos de autor.

Queda expresamente prohibido acceder o instalar programas obtenidos a través del Internet, aunque sean gratis, de prueba o por tiempo. De igual forma, se prohíbe utilizar el Internet para copiar, acceder o enviar programas protegidos por las leyes de derecho de autor.

En la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de

Gerencia y Presupuesto, se establece que cada entidad gubernamental utilizará sistemas de protección contra virus y sistemas de protección contra accesos no autorizados (*firewall*).

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05*, se establece que las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados, tales como: virus, *spyware*⁶, *adware*⁷ y *updates* automáticos.

El uso de las computadoras y de las cuentas para acceder a Internet y al correo electrónico de la Autoridad para procesar documentos y examinar archivos de carácter privado es contrario al interés público y desvirtúa los propósitos para los cuales fueron adquiridas. Además, provee al funcionario o empleado que indebidamente las utiliza, ventajas, beneficios y privilegios que no están permitidos por ley. Por otro lado, los programas no autorizados y los archivos ajenos a la gestión pública ocupan espacio y capacidad en los sistemas de información, lo que afecta el rendimiento de los mismos. Además, proliferan la transmisión de los virus de computadoras, lo que podría destruir información importante almacenada en las mismas. [**Apartado del a.1) al 4)**]

La situación comentada en el **Apartado a.5)** impide la prevención y la detección de programas no deseados, y da lugar a que éstos se propaguen en los sistemas de información, lo que podría afectar la integridad, la confidencialidad y la disponibilidad de éstos.

La situación comentada en el **Apartado a.6)** propicia la instalación y el uso de programas no autorizados, según se comenta en el **Apartado a.4)**, y la remoción de programas autorizados, con los consiguientes efectos adversos.

⁶ Programa que se instala inadvertidamente en una computadora y que propaga, sin autorización, información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

⁷ Programa que se instala inadvertidamente en una computadora para desplegar ante el usuario anuncios y propagandas.

Las situaciones comentadas se debían a la falta de:

- Orientaciones periódicas a los usuarios de los equipos computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de las computadoras, el correo electrónico e Internet. **[Apartado del a.1) al 4)]**
- Controles efectivos para asegurarse del uso oficial de los sistemas computadorizados y de las cuentas de acceso a Internet, y para la detección, el control y la corrección de virus o programas no deseados. **[Apartado del a.1) al 5)]**
- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento por los usuarios de las normas establecidas sobre el uso oficial de las computadoras y de las cuentas para acceder a Internet y al correo electrónico. **[Apartado del a.1) al 4)]**
- Controles efectivos que limiten el acceso a la opción de *Add/Remove Programs* del sistema operativo en las computadoras. **[Apartado a.6)]**

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Se incorporó en el Plan de Trabajo de la Oficina de Sistemas de Información (OSI) una revisión de todas las computadoras de la agencia con el propósito de eliminar todo documento ajeno a la gestión pública. **[Apartado a.1)]**

Se envió una comunicación a todos los usuarios en donde se cita los siguientes documentos al respecto: **[Apartado a.2) y 3)]**

- Sección 9 del Artículo VI de la Constitución del Estado Libre Asociado de Puerto Rico.
- El Artículo 3.2 de la Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental

- Carta Circular Núm. 2003-01 Para Establecer la Política de la Autoridad de Desperdicios Sólidos en cuanto al Uso, Manejo Adecuado del Internet y el Uso y Manejo Adecuado del correo electrónico (Carta circular 2003-01) [sic]

Se incorporó en el Plan de Trabajo de la Oficina de Sistemas de Información (OSI) una revisión de los programas instalados en cada computadora con el propósito de desinstalar aquellos programas que no guarden relación con las gestiones de la Autoridad. Además, se enviará un comunicado a todos los usuarios en donde se cita los siguientes documentos al respecto: [**Apartado a.4**]

- Carta Circular Núm. 2003-01 Para Establecer la Política de la Autoridad de Desperdicios Sólidos en cuanto al uso, manejo y conservación de las computadoras: el Uso y Manejo Adecuado del Internet y el Uso y Manejo Adecuado del correo Electrónico (Carta Circular 2003-01)

Se incorporó en el Plan de Trabajo de la Oficina de Sistemas de Información (OSI) una revisión de los programas instalados en cada computadora con el propósito de instalar un programa de antivirus en aquellos equipos que no lo tengan. Se estará impartiendo las instrucciones al Administrador de la Red para que revise periódicamente los programas de antivirus en cada computadora. [sic] [**Apartado a.5**]

Se estará impartiendo las instrucciones al Administrador de la Red para que revise los accesos otorgados a los usuarios de forma que se le limite el acceso a la opción de ADD/Remove Programs sin afectar la ejecución de programas que requieren mayor acceso de parte del usuario. [sic] [**Apartado a.6**]

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

Hallazgo 2 - Falta de controles relacionados con los equipos computadorizados

- a. Del 11 de diciembre de 2007 al 12 de febrero de 2008, examinamos 25 computadoras ubicadas en las distintas oficinas de la Autoridad. En 6⁸ de éstas (24 por ciento), determinamos discrepancias en cuanto a su localización física y la indicada en el *Asset Listing Report* provisto por la Autoridad el 7 de noviembre de 2007.

⁸ Véase la nota al calce 4.

- b. El Edificio de Agencias Ambientales (Edificio) alberga al Departamento, a la Junta de Calidad Ambiental y a la Autoridad. El examen realizado el 15 de enero de 2008 a los cuartos de cableado de la Autoridad y al área de los servidores reveló que a cuatro⁹ *switches*¹⁰ no se les había asignado un número de propiedad ni identificado como propiedad de ésta. Tampoco estaban incluidos en el *Asset Listing Report*.
- c. Al 7 de febrero de 2008, no se había localizado para examen una computadora portátil¹¹ adquirida el 30 de mayo de 2002. Según la información del *Asset Listing Report* de la Autoridad, esta computadora estaba asignada al Gerente de Sistemas de Información de la OSI.

En el Artículo 10(a) de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, se establece que la custodia, el cuidado y el control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia o entidad corporativa o su representante autorizado.

En el *Reglamento para Uso, Control y Disposición de Propiedad Mueble* se establecen las normas que rigen el uso, el control y la custodia de la propiedad de la Autoridad. En el Artículo VIII del mismo se dispone que el Encargado de la Propiedad será responsable de:

[...]

- d. Asignarle número de propiedad y marcarlo, adheriéndole la laminilla al mueble y equipo nuevo adquirido por la Autoridad, ya sea éste comprado, donado o transferido. [*sic*]

[...]

⁹ Los números de serie, la marca y el modelo de estos *switches* se incluyeron en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al ex Secretario de Recursos Naturales y Ambientales, y al Director Ejecutivo y al ex Director Ejecutivo de la Autoridad.

¹⁰ Dispositivo de comunicación central que conecta dos o más segmentos de red y permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

¹¹ Véase la nota al calce 4.

g. Visitar periódicamente a las unidades, áreas, divisiones o empleados para verificar lo que indica el inventario de propiedad y la hoja de propiedad en uso.

h. Corregir el registro o listado de propiedad periódicamente, de acuerdo a las bajas, transferencias y localización de la propiedad mueble. [*sic*]

[...]

j. Realizar un inventario de propiedad bajo su control cuando lo estime necesario y que no exceda de los seis (6) meses.

También se establece que el número de propiedad asignado aparecerá en el inventario de propiedad, el cual debe estar reconciliado con el Mayor General de la Oficina de Contabilidad.

En el Artículo IX del *Reglamento* se establece que todo empleado de la Autoridad a quien se le asigne mueble o equipo (custodio) es responsable de:

[...]

d. Informar al Encargado de la Propiedad siempre que se efectúe una transacción de mueble y equipo, ya sea por transferencia o retiro.

Las situaciones que se comentan en los **apartados a. y b.** no permiten a la Autoridad mantener un control adecuado de la propiedad, lo que podría propiciar el uso indebido o la pérdida de la misma, sin que se puedan detectar a tiempo para fijar responsabilidades. Además, dificultan la identificación y la localización de los equipos y le resta confiabilidad a la información existente en el sistema de inventario de activos. También dificultan nuestra gestión fiscalizadora.

La situación comentada en el **Apartado c.** impidió que nuestros auditores examinaran el equipo para verificar el uso y el estado en que el mismo se encontraba.

La situación comentada en el **Apartado a.** se debió a que el Encargado de la Propiedad de la Autoridad y el personal que tenía asignado el equipo no cumplieron con las disposiciones sobre el control de los equipos computadorizados establecidas en el *Reglamento*.

La situación comentada en el **Apartado b.** se debió a que la Supervisora del Área de Compras de la Autoridad no le impartió instrucciones al Encargado de la Propiedad de la Autoridad para que asignara un número de propiedad a dichos equipos. Además, los jefes de las agencias mencionadas no habían definido el método de distribución de ese equipo, para incluirlo en el inventario de la propiedad de cada una de éstas o en el de la Autoridad.

Con respecto a la situación comentada en el **Apartado c.**, el Encargado de la Propiedad de la Autoridad alegó que se debía a un error que se cometió durante el proceso para decomisar el equipo realizado en mayo de 2005. Durante el mismo, se anotó en el formulario *Solicitud para Bajas de Propiedad (ADS-42-005)* una computadora con un número de propiedad¹²; sin embargo, se decomisó otra que se identificó con otro número de propiedad.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informo, entre otras cosas, lo siguiente:

Como parte de los procedimientos de la auditoría financiera del año fiscal terminado el 30 de junio de 2009 a la ADS, se realizó un inventario físico de todos los equipos de la ADS. En el inventario se revisó la existencia de cada uno de los equipos registrados en el Mayor General. También se revisó cada área de la ADS para verificar que todo equipo propiedad de la ADS esté debidamente registrado e identificado, así como la localización exacta del mismo. **[Apartado a.]**

Se envió una comunicación al Área de Servicios Generales indicándole la situación encontrada en la auditoría realizada para que se tomen las medidas correspondientes para resolver la situación. *[sic]* **[Apartado b.]**

¹² Una computadora con este número de propiedad se localizó en la OSI de la Autoridad.

Se le envió una comunicación al Área de Servicios Generales aclarando la situación expuesta en el hallazgo. De la misma forma se le indicó se tomen las medidas necesarias para evitar que la situación descrita no se repita. [sic] **[Apartado c.]**

Véanse las recomendaciones 1 y de la 4 a la 6.

Hallazgo 3 - Normas y procedimientos importantes no incluidos en la reglamentación aprobada para la seguridad y el uso de los sistemas de información computadorizados, y falta de normas y de procedimientos escritos para la instalación y la configuración de la red

- a. El examen del contenido de la *Carta Circular Núm. 2003-01* y de la *Advertencia para el uso del Sistema de Información Computadorizado* instalada en las computadoras de la Autoridad reveló que las mismas no contenían normas y procedimientos importantes para:
- 1) Orientar al usuario sobre la prohibición de lo siguiente:
 - El uso de medios de almacenaje de información no certificados libre de virus
 - El uso de protectores de monitores que podían resultar poco serios u ofensivos
 - La creación o el envío de archivos mediante el correo electrónico que excedan la capacidad de espacio en disco asignado al usuario en el servidor
 - El uso de programas de charlas (*Chats*) no autorizados expresamente por la agencia.
 - 2) Establecer que las normas serán revisadas periódicamente.
- b. Al 28 de noviembre de 2007, no se habían establecido normas y procedimientos para la instalación y configuración de la red.

En el Artículo 10 del *Plan de Reorganización Núm. 1 de 1993* se dispone que el Secretario de Recursos Naturales y Ambientales, entre sus funciones, tiene que administrar y ejercer las funciones normativas y reglamentarias para todo el Departamento y sus componentes.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establecen las directrices generales que permiten a las agencias establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Se indica que cada entidad gubernamental tiene la responsabilidad de desarrollar normas específicas de seguridad que consideren las características propias de los ambientes de tecnología de ésta, particularmente, sus sistemas de misión crítica.

En la *Política Núm. TIG-008* de dicha *Carta Circular* se establece que cada agencia debe establecer políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y estén aprobadas por la alta gerencia. Mediante los mismos se logra definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones, en casos de renunciaciones o ausencias del personal de mayor experiencia, y facilitan la labor de adiestramiento.

Las situaciones comentadas propician que los mecanismos de control y las operaciones de la Autoridad no se realicen de manera uniforme. Esto puede reducir la efectividad de los sistemas computadorizados y afectar la continuidad de las operaciones. Además, expone la información a riesgos innecesarios y promueve el uso indebido de los equipos computadorizados.

La situación comentada en el **Apartado a.** se debe, en parte, a que el Director Ejecutivo de la Autoridad no incluyó los requisitos de seguridad y de administración de los sistemas de información computadorizados mencionados cuando emitió las normas.

La situación comentada en el **Apartado b.** se atribuye, principalmente, a que el Director Ejecutivo de la Autoridad no le había requerido al Gerente de Sistemas de Información de la OSI que desarrollara y remitiera para su consideración, y para la aprobación del Secretario de Recursos Naturales y Ambientales, las normas y los procedimientos para reglamentar los referidos procesos.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Se estarán redactando enmiendas a la Carta Circular Núm. 2003-01 para que incluya los siguientes: *[sic]* [**Apartado a.1)**]

- El uso de medios de almacenamiento de información no certificados libre de virus
- Utilizar protectores de monitores (Screen Saber) que puedan resultar poco serios u ofensivos. *[sic]*
- El establecimiento de un límite en el envío y recibo de correos electrónicos.
- El uso de programas de charlas (chats)

Se incorpora en el Plan de Trabajo el realizar un estudio para la definición del tamaño máximo en el envío y recibo de mensajes de correo electrónico.

Se estipulará en la enmienda a la Carta Circular Núm. 2003-01 que dichas normas serán revisadas periódicamente y de ser necesario se harán los cambios pertinentes. [**Apartado a.2)**]

Para este año se incorpora y establece en el Plan de Trabajo de los Sistemas de Información el desarrollo de las normas y procedimientos a seguir en la instalación y configuración de la red de comunicaciones. Se estará utilizando la Política Núm. TIG de la Carta Circular Núm. 77-05 como guía para el desarrollo de las normas y procedimientos. *[sic]* [**Apartado a.3)**]

Véanse las recomendaciones 1, 2 y 3.f.

Hallazgo 4 - Deficiencia relacionada con la Certificación de Recibo, Aceptación y Conocimiento de Medidas Disciplinarias, y faltas de control de la misma

- a. El formulario *Certificación de Recibo, Aceptación y Conocimiento de Medidas Disciplinarias (Certificación)* se utiliza para que cada empleado certifique que recibió de su supervisor, copia de las normas para establecer la política de la Autoridad en cuanto al uso, al manejo y a la conservación de las computadoras, del Internet y del correo electrónico (*Carta Circular Núm. 2003-01*). La Oficina de Recursos Humanos de la Autoridad mantiene las *certificaciones* completadas en el expediente de cada empleado. En el examen de este formulario encontramos que en el mismo no se requería la firma del Supervisor del empleado como evidencia de que le había suministrado la *Carta Circular Núm. 2003-01* a éste.
- b. El examen del control de las *certificaciones* de los 14 usuarios de las 15 computadoras examinadas según el **Hallazgo 1** reveló lo siguiente:
 - 1) Cuatro¹³ (29 por ciento) no se encontraron ni los funcionarios suministraron las mismas.
 - 2) Tres¹³ (21 por ciento) no estaban firmadas por los usuarios.

En un memorando, emitido el 9 de mayo de 2003 por el Director Ejecutivo a todo el personal de la Autoridad, se indicó que se iba a distribuir a cada empleado un formulario, que se incluiría con la *Carta Circular Núm. 2003-01*, el cual debía ser firmado por el empleado y el supervisor de éste. Una vez completado el formulario, éste se debía remitir a la Oficina de Recursos Humanos de la Autoridad.

En la *Política Núm. TIG-008 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad, y de las herramientas de Internet

¹³ Una relación de los usuarios se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al ex Secretario de Recursos Naturales y Ambientales y al Director Ejecutivo y al ex Director Ejecutivo de la Autoridad.

y de correo electrónico. En ésta se indicarán los usos permitidos, los no permitidos y las sanciones o medidas disciplinarias que se aplicarían a los usuarios que incumplieran con la misma. Asimismo, será responsabilidad de cada entidad particular notificar debidamente a los empleados del contenido de la misma. Los usuarios, a su vez, firmarán un documento que indique que conocen la política y que cumplirán con ella.

Las situaciones comentadas podrían causar que los usuarios de los equipos y de los sistemas computadorizados de la Autoridad no observen las normas principales sobre el uso de éstos, por lo que se dificulta imponer sanciones por la violación a las mismas, y provocan que se incurra en irregularidades y otras situaciones adversas.

Las situaciones comentadas se debieron a que la Directora de la Oficina de Recursos Humanos no se aseguró de que a todos los empleados de la Autoridad se les entregara la *Carta Circular Núm. 2003-01*, que la *Certificación* tuviera la firma del empleado y que se requiriera la firma del Supervisor. Tampoco se aseguró de que la *Certificación* se guardara en el expediente de los empleados.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Se le envió una comunicación al Director de Recursos Humanos donde se le indicó la situación encontrada durante la auditoría de los Sistemas de Información relacionada a la entrega de la Carta Circular Núm. 2003-01. Esto con el propósito de que se asegure que todos los empleados hayan recibido la Carta Circular en referencia y firmen el Certificado de Recibo, Aceptación y Conocimiento de Medidas Disciplinarias. [sic] [**Apartados a. y b.**]

Véanse las recomendaciones 1, 7 y 8.

Hallazgo 5 - Deficiencias en los cuartos de distribución del cableado (*wiring closets*) de la red y en el área de los servidores del Centro de Cómputos

- a. El examen efectuado el 15 de enero de 2008 al área de los servidores y a los tres cuartos de distribución del cableado (*wiring closets*) de la red de la Autoridad, reveló las siguientes deficiencias:
- 1) Ninguno de los cuartos de cableado tenía un diagrama de los *drops*¹⁴.
 - 2) El área de los servidores ubicado en el Centro de Cómputos, y dos de los tres cuartos de cableado examinados, no cumplían con las condiciones ambientales adecuadas para proteger los equipos de comunicaciones. En éstos se almacenaban materiales inflamables, tales como: cajas de cartón vacías y cajas con cables de transmisión de datos, rollos de cable de teléfono, equipo, y materiales de construcción y de limpieza.
 - 3) Los equipos de comunicaciones de los tres cuartos de cableado no estaban conectados a un generador de energía ininterruptionable (*UPS*, por sus siglas en inglés), para protegerlos contra cambios repentinos en la energía eléctrica.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica, de la Carta Circular Núm. 77-05*, se establece que las agencias tendrán la responsabilidad de adquirir 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. También se establece que las redes en las agencias deben proveer la infraestructura necesaria para implementar y mantener los procesos de negocio de la agencia, y ser operacionales y confiables.

¹⁴ Conector de pared para instalaciones de redes.

Las mejores prácticas en el campo de la tecnología de información sugieren que para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados es necesario que:

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red, de forma que se puedan corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada.
- No se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos.
- Los equipos de comunicaciones tengan la protección eléctrica adecuada.

La situación comentada en el **Apartado a.1)** impide a la Autoridad obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

La situación comentada en el **Apartado a.2)** pudiera ocasionar daños y deterioros prematuros a los equipos de la red, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos.

La situación comentada en el **Apartado a.3)** pudiera ocasionar daños en los equipos de comunicaciones y la pérdida de información por interrupciones o fluctuaciones en la energía eléctrica.

Las situaciones comentadas se debieron a que el Gerente de Sistemas de Información de la OSI:

- No le había requerido a la compañía consultora, a cargo de la infraestructura de telecomunicaciones del proyecto del Edificio, un diagrama de los *drops* de los cuartos de distribución del cableado de la Autoridad [**Apartado a.1)**]

- No había cumplido con los parámetros de seguridad establecidos en las mejores prácticas de sistemas de información para mantener los equipos de comunicaciones de los cuartos de cableado conectados a un *UPS*. [**Apartado a.3**]

En cuanto al **Apartado a.2)**, el Gerente de Sistemas de Información de la OSI le indicó a nuestros auditores que la situación obedecía a que la estructura del edificio carecía de espacio para guardar los materiales mencionados. Además, el personal de las compañías a cargo de la infraestructura de la red y de proveer los servicios telefónicos al finalizar sus trabajos dejaban el material no utilizado y cajas vacías en los cuartos de cableado.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Por razones de seguridad, no se mantiene un diagrama detallado de la distribución del cableado en los cuartos de cableado. Dichos diagramas estarán incluidos en el Manual de configuración a ser almacenado en la Oficina de Sistemas de Información. Además, por seguridad, el mismo solo estará disponible a personal autorizado. [*sic*] [**Apartado a.1**]

Se le notificó al Área de Servicios Generales sobre la situación encontrada de las condiciones ambientales dentro del área del centro de Cómputos. Conjuntamente se le solicitó a que procedan a remover todo material y equipo que no esté relacionado con los equipos de comunicaciones. Además, se les envió una comunicación a los encargados de las agencias que comparten el cuarto de servidores para que remuevan todo material o equipo no relacionado a dicho cuarto de servidores. [**Apartado a.2**]

Consideramos las alegaciones de la Directora Ejecutiva de la Autoridad con respecto al **Apartado a.1) del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones 1 y 3.g.

Hallazgo 6 - Falta de adiestramientos periódicos al Administrador de la Red de la Autoridad

a. El Analista Programador, quien funge como Administrador de la Red de la Autoridad, no recibía adiestramientos continuos sobre los temas relacionados con sus funciones, tales como:

- Sistemas operativos
- Protocolos de la red
- Diseño, instalación, configuración y mantenimiento de la red
- Monitoreo de la red, herramientas para la autoevaluación de la misma y detección de intrusos
- Análisis de problemas
- Novedades, actualizaciones o mejoras en los sistemas
- Nuevas amenazas y posibles soluciones
- Productos que podrían implantarse o se implantarán en la red antes de que se realicen los cambios
- Seguridad y confidencialidad de la información, y de las leyes de derecho de autor de los programas computadorizados.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, lo siguiente:

- La agencia es responsable de proveer adiestramientos a toda la gerencia y los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

- El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.
- La agencia es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

La situación comentada podría reducir la efectividad de los sistemas computadorizados y exponer los datos a riesgos innecesarios que afecten la continuidad de las operaciones de la Autoridad.

La situación comentada se debe a que el personal de la OSI de la Autoridad sólo recibe adiestramientos que sean libres de costo. Esto, debido a que la Autoridad no cuenta con los fondos suficientes para sufragar las necesidades de adiestramiento continuo para el Administrador de la Red.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Se estarán identificando las áreas de necesidad de adiestramientos para establecer un programa de adiestramiento continuo. [sic]

Se coordinará con la Oficina de Recursos Humanos el proceso de adiestramiento. Para ello se le estará solicitando a la Oficina de Recursos Humanos la lista de adiestramientos de forma regular con el propósito de realizar las gestiones necesarias para el envío del personal a los mismos. [sic]

Véanse las recomendaciones 1 y 9.

Hallazgo 7 - Deficiencias relacionadas con la documentación de la configuración de las instalaciones de la red

- a. La documentación de la estructura de la red, suministrada para examen durante nuestra auditoría, no contenía la siguiente información:
 - Un diagrama esquemático que permitiera identificar las conexiones y el cableado de la red.

- La descripción, instalación y configuración del equipo de comunicación ubicado en los cuartos de distribución del cableado de los diferentes pisos de la Autoridad.
- El detalle de las computadoras conectadas a la red, con sus respectivas identificaciones y localizaciones.
- La instalación y configuración del sistema operativo de cada computador principal conectado a la red, y de las aplicaciones utilizadas en la Autoridad.

En la *Política Núm. TIG-011 de la Carta Circular 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar 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 la red en funciones aceptables es necesario establecer controles adecuados de los inventarios, la ubicación y las conexiones entre sus componentes. Esto se logra mediante la documentación detallada y actualizada de las conexiones que permita corregir, a tiempo, los problemas de comunicación de la red y detectar cualquier conexión no autorizada.

La situación comentada impide a la Autoridad tener una comprensión clara y precisa de los componentes de la red, y dificulta mantener un control eficiente y efectivo en la administración y el mantenimiento de la misma. También dificulta atender los problemas de conexión en un tiempo razonable y planificar efectivamente las mejoras a la red, según el crecimiento de sus sistemas.

La situación comentada se debe a lo siguiente:

- La compañía consultora a cargo de la infraestructura de telecomunicaciones del proyecto del Edificio de Agencias Ambientales, no había completado sus servicios ni entregado a la Autoridad el proyecto finalizado con la documentación correspondiente a la estructura y configuración de la red.

- La instalación del sistema operativo y de las aplicaciones principales utilizadas en la Autoridad y la configuración de los equipos de telecomunicaciones conectados a la red se consideraban interactivas, por lo cual consideraban innecesario documentar las mismas.

La Directora Ejecutiva de la Autoridad, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Actualmente, se están realizando las gestiones para la adquisición de un sistema de inventario de computadoras para el desarrollo de listados detallados de las configuraciones de toda la red. Entre las alternativas revisadas se está evaluando la adquisición de un programa "Open Source". [*sic*]

Véanse las recomendaciones 1, y 3.h. e i.

ANEJO

**AUTORIDAD DE DESPERDICIOS SÓLIDOS EN PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Javier Vélez Arocho	Secretario de Recursos Naturales y Ambientales	1 jun. 07	30 abr. 08
Dr. Javier A. Quintana Méndez	Director Ejecutivo	1 jun. 07	30 abr. 08
Lcda. Irma M. Pagán Villegas	Subdirectora Ejecutiva	1 jun. 07	30 abr. 08
Sr. Alvin Román Lugo	Director de Asuntos Gerenciales ¹⁵	16 jun. 07	30 abr. 08
Sra. Vanesa Villafañe Riera	Directora de Recursos Humanos	1 jun. 07	30 abr. 08
Sr. Luis M. Cruz López	Director de la División de Servicios Generales Interino ¹⁶	9 jul. 07	30 abr. 08
Sr. Alvin Román Lugo	Director de la División de Servicios Generales	1 jun. 07	15 jun. 07
Vacante	Oficial Principal de Informática	1 jun. 07	30 abr. 08
Sr. William Mercado Rosado	Gerente de Sistemas de Información	1 jun. 07	30 abr. 08
Sr. Amílcar Torres Delgado	Auditor Interno	1 jun. 07	30 abr. 08

¹⁵ Puesto vacante del 1 al 15 de junio de 2007.

¹⁶ Puesto vacante del 16 de junio al 8 de julio de 2007.